

Docket No.: 17250/018001
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Jean-Luc Dauvois

22511
PATENT TRADEMARK OFFICE

Application No.: 10/538,725

Confirmation No.: 6778

Filed: June 13, 2005

Art Unit: N/A

For: METHOD FOR ACCESS CONTROL IN
DIGITAL PAY TELEVISION

Examiner: Not Yet Assigned

RENEWED PETITION UNDER 37 C.F.R. § 1.47(b)

MS PCT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In connection with the Applicant's response to the Decision on Petition ("Decision") mailed July 26, 2006, please consider the following renewed petition under 37 C.F.R. § 1.47(b).

In response to the Notice, Applicant submits two Declarations, the first made by Alexandra Dorotte, and the second made by Frédérique Dersoir, which detail attempts to contact the non-signing inventor, Jean-Luc Dauvois, by multiple communication means. Alexandra Dorotte is an employee of Osha · Liang LLP, who works in the European office located in Paris, France. Frédérique Dersoir is an employee of THOMSON who worked together with Isabelle Thibaudeau to obtain an executed Declaration from Jean-Luc Dauvois. THOMSON is affiliated with Nagra Thomson Licensing.

Both Alexandra and Frederique are persons with first-hand knowledge of the factual events surrounding attempts to obtain the non-signing inventor's executed Declaration. Specifically, the Declaration by Alexandra Dorotte sets forth the steps undertaken to contact

Jean-Luc Dauvois by registered mail and telephone. As required by the Decision mailed on July 26, 2006, the Declaration by Alexandra Dorotte includes a verification of the last known address for Jean-Luc Dauvois. In addition, the Declaration by Alexandra Dorotte establishes that inventor Jean-Luc Dauvois, or someone associated with Jean-Luc Dauvois, received the application as filed with the USPTO along with the corresponding Assignment and Declaration documents for execution that was mailed to Jean-Luc Dauvois at the verified last known address.

Further, the Declaration by Frédérique Dersoir sets forth the final step undertaken to contact Jean-Luc Dauvois via registered mail. The original communication and corresponding English translation are provided as attachments to Frédérique Dersoir's Declaration.

After diligent effort, Nagra Thomson Licensing, whom the petitioner represents, has been unable to obtain a signed Declaration from Jean-Luc Dauvois. The Declarations made by Alexandra Dorotte and Frédérique Dersoir establish that Jean-Luc Dauvois is an uncooperative inventor.

Canal+ Technologies has sufficient proprietary interest in the referenced application, as evidenced by the attached Declaration of Gerard Delile, a French attorney of competent jurisdiction. The Declaration made by Gerard Delile establishes that Jean-Luc Dauvois made the referenced invention while employed by Canal+ Technologies and that Canal+ Technologies rightfully owns the present invention under French law. Canal+ Technologies underwent a name change from Canal+ Technologies to Nagra Thomson Licensing on June 21, 2004 (*see* attached French document entitled "Assemblée Generale Mixte," and the corresponding English translation, page 2). The attached document establishes chain of title from Canal+ Technologies to Nagra Thomson Licensing. Thus, Nagra Thomson Licensing has sufficient proprietary interest in the referenced application.

In addition, attached is an executed Declaration signed on behalf of the non-signing inventor. The Declaration is executed by the Chief Executive Officer (CEO) of Nagra Thomson Licensing, Jan Steven Mes. The executed Declaration includes the CEO's signature, printed name, title, and the date, along with Jean-Luc Dauvois's correct last known address. The executed Declaration establishes that Nagra Thomson Licensing has the requisite ownership in the referenced application.

Applicant believes that this renewed petition, combined with the previously submitted evidence included in the original 37 C.F.R. § 1.47(b) petition filed on July 7, 2006, satisfy all the elements required under 37 C.F.R. § 1.47(b). In light of the petitioner's diligent attempts to obtain the signature of the inventors and, pursuant to 37 C.F.R. § 1.47(b), the petitioner requests that the referenced application be examined without the signed Declaration of Jean-Luc Dauvois. Such action is necessary to preserve the rights of the Applicant and to prevent irreparable damage which may be caused by the loss of foreign rights for the Applicant.

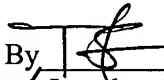
The verified last known address of Jean-Luc Dauvois is:

80 rue des Victimes du Nazisme, 72000 Le Mans, France.

We believe this petition addresses all outstanding issues raised in the Decision mailed on July 26, 2006. If this belief is in correct, please feel free to contact the undersigned. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 17250/018001).

Dated: February 26, 2007

Respectfully submitted,

By  #45,079
Jonathan P. Osha *THOMAS SCHLESER*
Registration No.: 33,986
OSHA · LIANG LLP
1221 McKinney St., Suite 2800
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)
Attorney for Applicant

Attachments (Declaration by Alexandra Dorotte)
(Declaration by Frédérique Dersoir)
(Declaration by Gerard Delile)
(Declaration signed on behalf of the inventor by C.E.O. of Nagra Thomson Licensing)
(“Assemblée Generale Mixte” establishing Chain of Title)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Jean-Luc Dauvois

Confirmation No.: 6778

Application No.: 10/538,725

Art Unit: Not Yet Assigned

Filed: June 13, 2005

Examiner: Not Yet Assigned

For: METHOD FOR ACCESS CONTROL IN
DIGITAL PAY TELEVISION

DECLARATION OF ALEXANDRA DOROTTE

1. I, Alexandra Dorotte, am over the age of eighteen years, of sound mind and competent to make this declaration. I work in the European Office of Osha Liang LLP as a paralegal. The facts stated herein are of my personal knowledge and I know them to be true and correct.
2. I am fluent in both French and English.
3. Jean-Luc Dauvois is the sole inventor of the following patent applications:
10/538,725; 10/510,533; 10/544,009.
4. Jean-Luc Dauvois's last known address, obtained from Thomson, is 80 rue Victimes du Nazisme 72000 LE MANS, France.
5. I verified the last known address using a French-based online phone book service. Based on the results of my search, the last known address for Jean-Luc Dauvois appeared to be correct. (See Tab 1; Tab 1 shows a printout of the search results for all entries with the last name of "Dauvois" in the 72000 zipcode).

6. I sent a registered letter on October 18, 2006, to Jean-Luc Dauvois at his last known address. The letter included a copy of the Patent Application as filed along with the Declaration and Assignment for each of the following patent applications: 10/538,725; 10/510,533; 10/544,009. A copy of the Registered Letter and a corresponding English translation is attached under Tab 2.
7. I received a first receipt from the post office indicating that the registered letter under Tab 2 was sent to Jean-Luc Dauvois's last known address on October 19, 2006. (*See* Tab 3 for a true and correct copy of the first receipt).
8. I received a second receipt from the post office indicating that the registered letter under Tab 2 was picked-up from the post office on October 23, 2006. (*See* Tab 4 for a true and correct copy of the second receipt).
9. On November 2, 2006, I called Jean-Luc Dauvois at the phone number listed in the search results under Tab 1.
10. During our phone conversation, Jean-Luc Dauvois denied receiving my letter of October 18, 2006. However, Jean-Luc Dauvois confirmed that he previously worked for Canal+ Technologies and that he was in fact the inventor of the following patent applications: 10/538,725; 10/510,533; 10/544,009. Further, Jean-Luc Dauvois indicated that he was not willing to sign any of the Declarations at this time.

I, Alexandra Dorotte, hereby declare that all statements made herein of my own knowledge are true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Signed this day 21, of February 2007.

DOROTTE
Alexandra Dorotte

Votre requête : DAUVOIS
LE MANS (SARTHE)

Ville en Direct

[plan](#), [vue aérienne](#), [météo](#), [trafic](#),
[webcam](#), [cinéma](#), [spectacles](#)



Min : 14°C
Max : 24°C

> Réponses en orthographe exacte

1 réponse(s)

(liste 1-1)

dans la localité ...

Eymeret-Dauvois Isabelle

80 r Victimes du Nazisme 72000 LE MANS

02 43 89 75 15

[Plan](#) | [Itinéraire](#) | [Vue aérienne](#) | [A proximité](#)

08 73 89 95 73



Demandez, c'est trouvé !

Nom

Prénom

Adresse

Localité

Département
ou région

Rechercher

121, Avenue Des Champs Élysées
75008 Paris • France
www.oshaliang.com

OSHA • LIANG

Telephone: +33 1 5357 2949
Facsimile: +33 1 5357 2948
paris@oshaliang.com

Paris, le 18 Octobre 2006

Monsieur Jean Luc DAUVOIS
80 rue Victimes du Nazisme
72000 Le Mans

Par courrier recommandé

Re: Documents de cession et pouvoir
Inventions « Pay television, method for revoking rights in such
a system, associated decoder and smart card, and message
transmitted to such a decoder », « Unique key computation to
encipher the data memories » et « Method for access control in
digital pay television »
Nos ref: 21345/089US1, 21345/091US1 et 21345/084US1

Cher Monsieur Dauvois,

Notre société nommée Osha Liang est responsable de la gestion de certaines
demandes de brevets de la société Thomson anciennement Canal+ Technologies aux Etats-
Unis, en Europe et dans d'autres pays. Vous avez travaillé comme inventeur dans les
inventions ci-dessus référencées pour Canal+ Technologies.

Pour compléter chaque demande de brevets aux Etats-Unis, nous avons besoin
de déposer une cession et un pouvoir. Vous trouverez ci-joint ces documents à nous retourner
dûment signés pour chaque invention dans les meilleurs délais, si possible avant le 10
novembre 2006.

Je vous remercie par avance pour votre coopération et je reste à votre
disposition si vous avez la moindre question.

Veuillez agréer, Monsieur, l'expression de mes salutations distinguées.



Alexandra Dorotte

P.J. : Trois documents de cession
Trois déclarations
Trois demandes de brevet telles que déposées aux Etats-Unis

BKW/BKW/AD



Houston - Silicon Valley - Paris

Osha Liang - European Patent Attorneys
S.A.R.L. au capital de 15000 euros — RCS Paris B 438260853 — TVA N° FR 48 438260853
Bank: Société Générale, Paris Champs Elysées, FRANCE
Account Nr 20629571 — IBAN FR76 30003 03330 00020629571 54 — SWIFT SOGEFRPP

TRANSLATION

121, Avenue Des Champs Élysées
75008 Paris • France
www.oshaliang.com

OSHA • LIANG

Telephone: +33 1 5357 2949
Facsimile: +33 1 5357 2948
paris@oshaliang.com

Paris, October 18, 2006

Monsieur Jean Luc DAUVOIS
80 rue Victimes du Nazisme
72000 Le Mans

By registered letter

Re: Assignment and declaration documents
Inventions « Pay television, method for revoking rights in such
a system, associated decoder and smart card, and message
transmitted to such a decoder », « Unique key computation to
encipher the data memories » et « Method for access control in
digital pay television »
Our ref: 21345/089US1, 21345/091US1 and 21345/084US1

Dear Mr. Dauvois,

Our company is responsible for the handling of some patent applications in the
USA, Europe and some other countries for our client Thomson, formerly Canal+
Technologies. You worked as inventor for Canal+ Technologies in the above-mentioned
inventions.

In order to complete each patent application in the USA, we need to file an
assignment and a declaration form. Please find enclosed these documents to be signed and
returned to us as soon as possible, preferably before **November 10, 2006**

Thank you in advance for your cooperation on this matter. I remain at your
disposal if you have any questions.

Yours sincerely

Alexandra Dorotte

Encl.: Three assignment documents
Three declaration documents
Three patent application as filed in U.S.A

BKW/BKW/AD



Houston - Silicon Valley - Paris

Osha Liang – European Patent Attorneys

S.A.R.L. au capital de 15000 euros — RCS Paris B 438260853 — TVA N° FR 48 438260853

Bank: Société Générale, Paris Champs Elysées, FRANCE

Account Nr 20629571 — IBAN FR76 30003 03330 00020629571 54 — SWIFT SOGEFRPP

Destinataire

Conservez ce feuillet, il sera nécessaire en cas de réclamation.
Le cas échéant, vous pouvez faire une réclamation dans
n'importe quel bureau de Poste.

SGR2 V2 D76 4A - M55.149 - 0506

Date

Prix

CRBT

Niveau de garantie :

8 € ☐ 153 € ☐ 458 € ☐

Número de l'envoi : RA 86 440 342 9 FR

RECOMMANDÉ AVEC AVIS DE RÉCEPTION

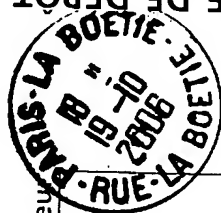
LA POSTE

Expéditeur

LA POSTE
19-10-2008
PARIS-LA BOETIE
RUE LA BOETIE
75008 PARIS



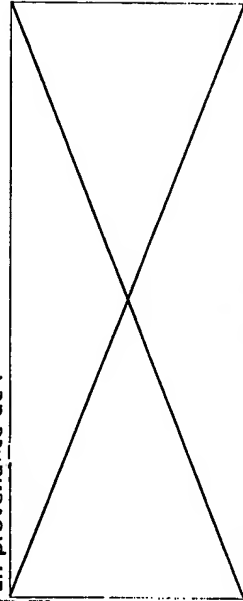
LA POSTE



PREUVE DE DÉPÔT
À CONSERVER PAR LE CLIENT

RCS PARIS 356 000 000

En provenance de :



Présentation le : 1 / 1 / 1
Distribution le : 1 / 1 / 1
Signature du destinataire ou du mandataire
(Précisez nom et prénom)

[Handwritten signature]

RCS PARIS 356 000 000

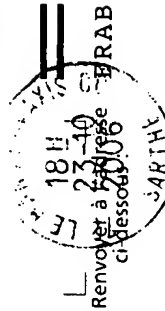
RECOMMANDÉ :
AVIS DE RÉCEPTION



LA POSTE

Numéro de l'envoi : RA 86 440 342 9 FR

21345/085 USA



OSHA - LIANG PARIS

Mme Zuno Wille
121 Av. des Champs Élysées
75008 PARIS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Jean-Luc Dauvois

Application No.: 10/538,725

Confirmation No.: 6778

Filed: June 13, 2005

Art Unit: N/A

For: METHOD FOR ACCESS CONTROL IN
DIGITAL PAY TELEVISION

Examiner: Not Yet Assigned

DECLARATION BY FRÉDÉRIQUE DERSOIR

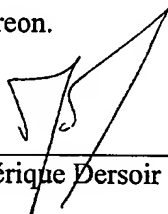
1. I, Frédérique Dersoir, am an employee of THOMSON, and hold the position of Patent Administration Manager.
2. I am responsible for providing our patent counsel in foreign countries with the necessary paperwork to file patent applications on behalf of THOMSON in their respective countries.
3. I am at least 21 years of age, I have firsthand knowledge of the facts set forth herein, and I am of sound mind and competent to make this declaration.
4. I am fluent in both French and English.
5. In the course of my duties, I worked with Isabelle Catinat-Thibaudeau in attempting to obtain a signed Declaration from inventor Jean-Luc Dauvois for U.S. Application Serial Nos. 10/538,725, 10/510,533, and 10/544,009.
6. I sent a letter to Jean-Luc Dauvois, at his last known address on February 6, 2007. The letter included, as attachments, the original applications as filed with the USPTO, as well as the corresponding Assignment and Declaration documents for Application Serial Nos. 10/538,725, 10/510,533, 10/544,009. See Tab 1 for a copy of the original French letter

and a corresponding English translation, as well as a true copy of the registered mail receipt.

7. In the letter, I confirmed that Jean-Luc Dauvois was unwilling to sign the Declarations for U.S. Application Serial Nos. 10/538,725, 10/510,533, 10/544,009, and stated that if we did not hear from Jean-Luc Dauvois within 7 business days, we would take this as evidence that he is uncooperative in this matter.
8. I have not heard from Jean-Luc Dauvois since sending the above letter, and 7 business days have passed.

I, Frédérique Dersoir, hereby declare that all statements made herein of my own knowledge are true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Signed this day 20nd, of February 2007.



Frédérique Dersoir

Frédérique Dersoir
Foreign Filing Manager
■ : 33 (0)1 41 86 52 70
☎ : 33 (0)1 41 86 56 33
✉ : frederique.dersoir@thomson.net

M. Jean-Luc DAUVOIS
80 rue des Victimes du Nazisme
72000 Le Mans

Boulogne, le 6 février 2007
FD/07.023

Lettre envoyée via DHL + Lettre recommandée avec A/R

N/Ref.: CPT02022/CPT02005/CPT03001

Objet : Demandes de brevet

US N°10/538,725 intitulée « Method for access control in digital pay television »
US N°10/510,533 intitulée « Method and device for protecting digital data stored in a memory »
US N°10/544,009 intitulée « Pay television, method for revoking rights in such a system, associated decoder and smart card, and message transmitted to such a decoder »

Monsieur,

Suite à nos courriels des 3 juillet, 17 mai et 5 mai 2006 relatifs aux demandes de brevet ci-dessus référencées respectives pour lesquelles vous êtes seul inventeur, nous comprenons que vous n'êtes pas disposé à signer les documents de Cession et Déclaration se référant à ces demandes.

Sans manifestation contraire de votre part dans les 7 jours ouvrables, il deviendra alors évident que vous n'êtes pas disposé à signer les documents de cession et déclaration des demandes de brevet ci-dessus référencées. Nous vous adressons un exemplaire de la demande telle que déposée ainsi que les documents de cession et déclaration correspondants pour chacune des demandes.

Frédérique DERSOIR

PJ. : Document de cession et de déclaration + Demande US (CPT02022/CPT02005/CPT03001)

TRANSLATION

Mr. Jean-Luc Dauvois
80 rue des Victimes du Nazisme
72000 Le Mans
FRANCE

Boulogne, February 6, 2007
FD/07.023

Via DHL and Registered Mail

N/Ref: CPT02005-CPT020022-CPT03001 - Jean Luc Dauvois

Subject: Patent Applications

US N°10/538,725 entitled " Method for access control in digital pay television"

US N° 10/510,533 entitled "Method and device for protecting digital data stored in a memory"

US N° 10/544,009 entitled "Pay television, method for revoking rights in such a system, associated decoder and smart card, and message transmitted to such a decoder"

Sir,

Further to our e-mails dated July 3, May 17 and May 5, 2006, with respect to the above referenced patent applications for which you are the sole inventor, we understand that you are unwilling to sign the Declaration and Assignment documents referring to these applications.

Unless we hear from you to the contrary within 7 business days, we will take this as evidence that you are unwilling to execute the Declaration and Assignment documents for these above referenced patent applications. We enclose a copy of the application as filed along with the corresponding declaration and assignment for each application ."

Frédérique DERVOIR

Attachments : US Applications and Declarations for references
(CPT02022/CPT02005/CPT03001)

LA POSTE

Destinataire

M. Jean LUX DAUVOIS
Identité ou raison sociale
80 rue des Victimes du
Nazisme
Adresse
72010101 LE MANS
Code postal
Commune

Présentation le : / /
Distribution le : / /
Signature du destinataire ou du mandataire
(Précisez nom et prénom)

Date : Prix : CRBT :
Niveau de garantie (valeur au dos) : R1 ☐ R2 ☐ R3 ☐

Cadres réservés à La Poste

SGR 2 VI MS R 01
05-10330-03 01-06

RECOMMANDÉ AVEC AVIS DE RÉCEPTION

Numéro de l'envoi : RA 56 501 806 6 FR
[Barcode]

Expéditeur
THOMSON (F. PERSOIR)
Identité ou raison sociale
European Patent Operations
N° 46
Quai A. Le Gall
Libellé de la voie
921648 BOULOGNE CEDEX
Code postal
COMMUNE

PREUVE DE DISTRIBUTION

PREUVE DE DEPOT
A CONSERVER PAR LE CLIENT

Utiliser uniquement un STYLO A BILLE en appuyant fortement

LETTRE

RCS PARIS 356 000 000

UNITED STATES PATENT
AND TRADEMARK OFFICE

**IN THE MATTER OF U.S PATENT
APPLICATIONS**

- **Serial N° 10/538,725, filed on 06/13/2005**
FIRST NAMED APPLICANT : Jean-Luc Dauvois
INTERNATIONAL APPLICATION N°
PCT/FR2003/045181
Filing date : 12/16/2003
Priority date 12/17/2002

- **Serial N° 10/510,533, file on 10/07/2004**
FIRST NAMED APPLICANT : Jean-Luc Dauvois
INTERNATIONAL APPLICATION N°
PCT/FR2003/01024
Filing date : 04/02/2003
Priority date 04/08/2002

- **Serial N° 10/544,009, filed on 08/01.2005**
FIRST NAMED APPLICANT : Jean-Luc Dauvois
INTERNATIONAL APPLICATION N°
PCT/EP2004/050060
Filing date : 01/30/2004
Priority date 02/04/2003

**DECLARATION OF GERARD
DELILE**

GERARD DELILE, declares pursuant to 28 U.S.C. § 1746, as follows:

1. I am an attorney in good standing practicing in France at the law firm of SCP SALANS & ASSOCIES of which I am a partner. I was admitted in the Paris bar in 1978, after having practiced as a "Conseil juridique" from 1966 until 1978. I am registered as a Foreign Lawyer with the Law Society of England and Wales (1999).

2. I have obtained a Maîtrise en Droit Privé (1966) and a Diplôme d'Etudes Supérieures de Droit Privé (1968) from the Law School of the University of Paris. I am certified as a Specialist in Intellectual Property Law (1994) and in the Law of International Relations (1994).

/.

3. I am listed as Expert in Industrial Property at the French Patent and Trademark Office ("PTO") under the headings "Lawyer" and "Trademarks and Designs" (1993). I am a member of the panel of examiners for the final professional examination to qualify as "Conseil en Propriété Industrielle" (Patent and Trademark Attorney) organized by the French PTO (2000 to date).

4. Member: National Council of the Bars (1992-1996); Association Française des Praticiens du Droit des Marques et des Modèles (APRAM, member of the Board); International Trademark Association (INTA, member of the Amicus Curiae Committee 2003 to date); Association des Avocats de Propriété Industrielle (AAPI, President 2007 to ____); National Anti-Counterfeiting Committee ("Comité National Anti-Contrefaçon", 2003 to date).

5. I have been practicing Intellectual Property Law, and in particular patent law, since 1966 both as a counselor and as a litigator.

6. It is my understanding that this Memorandum may be submitted in the matter of the below U.S patent Applications:

- Serial N° 10/538,725 (hereafter "US Application N° 1") filed on June 13, 2005 under the title "Method For Access Control In Digital Pay Television" with Jean-Luc Dauvois being named as first Applicant, following International Application N° PCT/FR2003/045181 filed on December 16, 2003 in the name of CANAL + TECHNOLOGIES, 34 Place Raoul Dautry, F – 75015 Paris, France, under the title "Method For Access Control in Digital Pay Television" naming Mr. Jean-Luc Dauvois,

./.

19 rue Eugène Manuel, F-75116 Paris, France as Inventor and, for the United States only as Inventor / Applicant,

- Serial N° 10/510,533 (hereafter "US Application N° 2") filed on October 7, 2004 under the title "Unique Key Computation To Encipher The Data Memories" with Jean-Luc Dauvois being named as first Applicant, following International Application N° PCT/FR03/01024 filed on April 8, 2002 in the name of CANAL + TECHNOLOGIES, 34 Place Raoul Dautry, F – 75015 Paris, France, under the title "Method And Device For Protecting Digital Data Stored In A Memory" naming Mr. Jean-Luc Dauvois, 19 rue Eugène Manuel, F-75116 Paris, France as Inventor and, for the United States only as Inventor / Applicant,

- Serial N° 10/544,009 (hereafter "US Application N° 3") filed on August 1, 2005 under the title "Pay Television System, Method For Revoking Rights In Such A System, Associated Decoder and Smart Card, And Message Transmitted To Such A Decoder" with Jean-Luc Dauvois being named as first Applicant, following International Application N° PCT/EP2004/050060 filed on January 30, 2004 in the name of CANAL + TECHNOLOGIES, 34 Place Raoul Dautry, F – 75015 Paris, France, under the title "Pay Television, Method For Revoking Rights In Such A System, Associated Decoder and Smart Card, And Message Transmitted To Such A Decoder" naming Mr. Jean-Luc Dauvois, 19 rue Eugène Manuel, F-75116 Paris, France as Inventor and, for the United States only as Inventor / Applicant,

(hereafter collectively "the US Applications").

./.

This Memorandum sets forth my opinion under French law as to the ownership of the inventions which are the subject matter of the US Applications (hereafter “the Inventions”).

I have been specifically asked to give a legal opinion as to (i) who of the employer or the employee is the owner of the unpatented inventions made in the course of his work by a salaried person hired especially to carry out technical researches, and (ii) whether such ownership is restricted to the territory of the French Republic or extends worldwide. It is my opinion, in light of the facts and generally accepted principles of the French patent law, that (i) the inventions belong to the employer, and (ii) that the employer's ownership is not limited to the French territory but it extends to all the countries throughout the world. In support of this opinion, I set forth, first the facts as they appear in the relevant documents which have been furnished to me, second, the applicable principles of the French patent law, and third, an analysis of the facts and of the law.

7. I have examined certain documents, including :

- (1) document in French entitled “Certificat De Travail” on Canal + Technologies stationery, dated « 06 septembre 2002 » (i.e. September 6, 2002) and signed by Sébastien Montet “Responsable Ressources Humaines” (i.e. Human Resource Manager), a copy of which is attached hereto with an English translation as **Exhibit 1**.
- (2) document in French entitled “Protocole Transactionnel” (i.e. Settlement Agreement) between Canal + Technologies and Mr. Jean-Luc Dauvois dated “13 juin 2002” (i.e. June 13, 2002) executed by Mr. Luc Germain on behalf of Canal + Technologies and by Mr. Jean-Luc Dauvois, a copy of which is attached hereto with an English translation as **Exhibit 2**.

./.

- (3) document entitled « Déclaration d'invention » on Canal + Technologies « Direction Juridique et Propriété Intellectuelle » stationery, hand dated « 9.5.01 » (i.e. May 9, 2001) and signed, a copy of which is attached hereto as **Exhibit 3**.
- (4) letter on Canal + Technologies stationery dated « 26 juin 2001 » (i.e. June 26, 2001) from Bruno Weihs to BREVALEX, a copy of which is attached hereto as **Exhibit 4**.
- (5) memorandum on Canal + Technologies stationery dated « 5 novembre 2001 » (i.e. November 5, 2001) from Bertrand Allain to Jean-Luc Dauvois, a copy of which is attached hereto as **Exhibit 5**.
- (6) letter on Canal + Technologies stationery dated « 12 novembre 2001 » (i.e. November 12, 2001) from Bertrand Allain to BREVALEX, a copy of which is attached hereto as **Exhibit 6**.
- (7) draft hand-annotated application for a French patent entitled “PROCEDE ET DISPOSITIF DE PROTECTION DE DONNEES NUMERIQUES STOCKEES DANS UNE MEMOIRE” hand dated “11.11.01” (i.e. November 11, 2001) signed and initialed “JLD”, a copy of which is attached hereto as **Exhibit 7**.
- (8) memorandum on Canal + Technologies stationery dated « 16 avril 2002 » (i.e. April 16, 2002) from Philippe Cassagne to Sébastien Montet, a copy of which is attached hereto as **Exhibit 8**.
- (9) letter on Canal + Technologies stationery dated « 23 avril 2002 » (i.e. April 23, 2002) from Philippe Duranton to Jean-Luc Dauvois, a copy of which is attached hereto as **Exhibit 9**.

/.

- (10) the first page of French patent application N° 02/15978 of December 17, 2002 a copy of which is attached hereto as **Exhibit 10**.
- (11) the first page of international patent application N° PCT/FR2003/045181 a copy of which is attached hereto as **Exhibit 11**.
- (12) the first page of French patent application N° 02/04321 of April 8, 2002 a copy of which is attached hereto as **Exhibit 12**.
- (13) the first page of international patent application N° PCT/FR03/01024 a copy of which is attached hereto as **Exhibit 13**.
- (14) the first page of French patent application N° 03/01243 of February 4, 2003 a copy of which is attached hereto as **Exhibit 14**.
- (15) the first page of international patent application N° PCT/EP2004/050060 a copy of which is attached hereto as **Exhibit 15**.
- (16) a series of fifteen international PCT (12) and US (3) patent applications and patents filed between 1997 and 2004 in the name of Canal + or Canal + Technologies with Jean-Luc Dauvois being named as inventor, alone or jointly with other(s), a copy of which is attached hereto as **Exhibit 16**.

I – FACTS

9. From July 17, 1995 up until September 6, 2002, Mr. Jean-Luc Dauvois (hereafter “Dauvois”) was employed first by Canal + and subsequently by Canal + Technologies, as a research engineer in electronics, information technologies and telecommunications, specializing in television related technologies, and notably in pay television, access control,

./.

secure transmission of data and information, data encryption, and information storage. He was the Head of the Encryption Department at Canal + Technologies. His duty was to carry out researches with a view to making inventions in these and in related or ancillary technological fields, Exhibits 1 and 9 hereto.

10. On June 13, 2002, in anticipation of Dauvois' leaving Canal + Technologies ("the Company") on September 7, 2002, the two parties entered into a settlement agreement whereby, in consideration for concessions made to him by the Company, Dauvois acknowledged notably, that :

"... in application of the article L 611-7 1°) of the CPI¹, [that] all the intellectual property rights to the inventions, in which Mr. Dauvois participated within the framework of the inventive missions that were entrusted to him during the years of his collaboration with the companies SECA and Canal + Technologies and particularly those that were filed and classified as an inventive mission, are the full and entire property of the Company and the remuneration stipulated in article 2.1 covers the remuneration stipulated in the said article.

Moreover, Mr. Dauvois also recognizes that in accordance with article L113-9 of the CPI, all the economic rights relating to all or part of the software applications (including their documentation), the production of which he participated in, are the exclusive property of the Company.

Mr. Dauvois agrees to perform at the earliest possible moment or to abstain from performing all that the Company could, if necessary, ask him to perform or to abstain from performing so as to enable the Company to be able to exercise the rights or to avail themselves, irrespective of the form, of the rights that Mr. Dauvois recognises above to be the property of the Company."

See Exhibit 2.

¹« CPI » = « Code de la Propriété Intellectuelle », i.e. Code of Intellectual Property

11. The invention which is the subject matter of US Application n° 1:

On December 17, 2002 an application for a French patent was filed in the name of Canal + Technologies under number FR02/15978, with Dauvois being named as inventor, see Exhibit 10.

On December 16, 2003 an international patent application was filed in the name of Canal + Technologies under number PCT/FR2003/050181 claiming priority of FR02/15978, naming Dauvois as Inventor and, for the United States only as Inventor / Applicant, see Exhibit 11, paragraphs (30), (71), (72), (75).

12. The invention which is the subject matter of US Application n° 2:

12.1 On or before May 9, 2001 Dauvois completed, signed and handed over to Bruno Weihs, a patent engineer at the Legal and Intellectual Property Department of Canal + Technologies, in charge of filing and prosecuting with the assistance of Brevaux, a firm of patent attorneys, the patent applications in the name of Canal + Technologies, a five page form of "Déclaration d'invention" (i.e a declaration of invention), Exhibit 3 hereto.

In the caption at the top right side one can read a date "9.5.01" and the internal reference of the file "12001.016".

In said declaration of invention Dauvois is named as an "employee" and "first inventor" of an invention called "Unique Key Computation To Encipher(ed) The Data Memories" (see Exhibit 3, p. 1, paragraph 1).

./.

The invention involved is described as “De mission” (see Exhibit 3, p. 1, paragraph 4).

12.2 On June 26, 2001 Mr Bruno Weihs sent the “Déclaration d’invention” to Brevalet and asked that a draft patent application be prepared with the assistance of Brevalet, Exhibit 4 hereto.

12.3 On November 5, 2001 Mr Bertrand Allain, General Counsel of Canal + Technologies, sent to Dauvois for his review and comments a draft French patent application prepared by Brevalet. The invention is entitled “Procédé et dispositif de protection de données numériques stockées dans une mémoire”(i.e. “Method And Device For Protecting Digital Data Stored In A Memory”) and the letter bears the same reference as in the “Déclaration d’invention”, i.e “I 2001.016”, Exhibit 5 hereto.

12.4 On November 12, 2001 Mr Bertrand Allain returned the draft patent application to Brevalet bearing hand-annotations by Dauvois, signed, initialed “JLD” and dated “11.11.01” by the latter, Exhibits 6 and 7.

12.5 On April 8, 2002 an application for a French patent was filed in the name of Canal + Technologies under number FR02/04321, with Dauvois being named as inventor, see Exhibit 12.

12.6 A few days after the filing of the application, Mr Philippe Cassagne (Head of Patents at Canal + Technologies), wrote on April 16, 2001 an internal memorandum to Mr Sébastien Montet (Head of Human Ressource at Canal + Technologies) advising him that Dauvois as inventor was entitled to an invention bonus of 5,000.00 French Francs (i.e.

./.

approximately 900.00 US dollars). Montet countersigned the memorandum on April 22, 2001 thus confirming his agreement to the payment of the 5,000.00 Francs bonus, Exhibit 8 hereto.

12.7 Shortly thereafter, on April 23, 2001, Mr Philippe Duranton (Deputy General Manager of Canal + Technologies + Technologies) wrote to Dauvois to advise him that in view of his part as inventor in the French patent application n° 02/04321 filed on April 8, 2001, he had been granted a bonus to the amount of 762.25 Euros (i.e. exactly 5,000.03 Francs), Exhibit 9 hereto.

12.8 On April 2, 2003 an international patent application was filed in the name of Canal + Technologies under number PCT/FR03/01024 claiming priority of FR02/04321, naming Dauvois as Inventor and, for the United States only as Inventor / Applicant, see Exhibit 13, paragraphs (30), (71), (72), (75).

13. The invention which is the subject matter of US Application n° 3:

On February 4, 2003 an application for a French patent was filed in the name of Canal + Technologies under number FR03/01243, with Dauvois being named as inventor, see Exhibit 14.

On January 30, 2004 an international patent application was filed in the name of Canal + Technologies under number PCT/EP2004/050060 claiming priority of FR0301243, naming Dauvois as Inventor and, for the United States only as Inventor / Applicant, see Exhibit 15, paragraphs (30), (71), (72), (75).

./.

14 As stated at the outset, the twofold question is (i) who of the employer or the employee is the owner of the unpatented inventions made in the course of his work by a salaried person hired especially to carry out technical researches, and (ii) whether such ownership is restricted to the territory of the French Republic or extends worldwide. The facts having been stated, I turn now to a consideration of the relevant principles of the French law of patents.

II – THE LAW

14. Under French patent law, in circumstances where an invention falls within the area of activity of an employee and the invention was made whilst the employee was working for the employer, the employee has no right in the invention, except that of being named as inventor. The invention belongs to the employer as of law.

Article L.611-7 of the French Code of Intellectual Property (« CIP »), reads as follows:

Article L.611-7 :

« Where the inventor is a salaried person, the right to the industrial property title, failing any contractual clause more favorable to the salaried person, shall be defined in accordance with the following provisions:

1°. Inventions made by a salaried person in the execution of a work contract comprising an inventive mission corresponding to his effective functions or of studies and research which have been explicitly entrusted to him, shall belong to the employer. The conditions under which the salaried person who is the author of such an invention shall enjoy additional remuneration shall be determined by the collective agreements, company agreements and individual employment contracts.

Where the employer is not subject to a sectorial collective agreement, any dispute relating to the additional remuneration shall be submitted to the joint conciliation board set up by Article L.615-21 or by the First Instance Court.

2°. All other inventions shall belong to the salaried person. However, where an invention made by a salaried person during the execution of his functions or in the field of activity of the company or by reason of knowledge or use of technologies or specific means of the company or of data acquired by the company, the employer shall be

./.

entitled, subject to the conditions and the time limits laid down by decree in *Conseil d'Etat*, to have assigned to him the ownership or enjoyment of all or some of the rights in the patent protecting his employee's invention.

The salaried person shall be entitled to obtain a fair price which, failing agreement between the parties, shall be stipulated by the joint conciliation board set up by Article L.615-21 or by the First Instance Court; these shall take into consideration all elements which may be supplied, in particular by the employer and by the employee, to compute the fair price as a function of both the initial contributions of either of them and the industrial and commercial utility of the invention.

3°. The salaried author of an invention shall inform his employer thereof and the latter shall confirm receipt in accordance with the terms and time limits laid down by regulation.

The salaried person and the employer shall communicate to each other all relevant information concerning the invention. They shall refrain from making any disclosure which would compromise, in whole or in part, the exercise of the rights afforded under this Book.

Any agreement between the salaried person and his employer concerning an invention made by the salaried person shall be recorded in writing, on pain of nullity.

4°. The implementing rules for this Article shall be laid down by decree in *Conseil d'Etat*.

5°. This Article shall also apply to the servants of the State, of local authorities and of any other public legal person under the terms to be laid down by decree in *Conseil d'Etat*. »

15. With the only exception of one decision rendered in 1986 by a lower court², both the Commission Nationale des Inventions de Salariés CNIS³ and the Courts of

² District Court ("Tribunal de Grande Instance") of Toulouse, 04.14.1986: PIBD 1986-III-290, Sté Formica v. Vidaillan. Commentators have strongly criticized this judgment, see: Dossier Brevets, 1986, VI, n° 2, p. 5, directed by Professor Jean-Marc Mousseron : "Consequently, the solution given by the Court of Toulouse is regrettable all the more so since it was pointless in the context. As a matter of fact, it would seem from certain expressions used by the Court that the latter did not fully master patent law".

³ Article L. 615-21 CIP introduced a procedural option, which allows an employer and an employee in dispute over an invention made by a salaried person, to decide to go through a preliminary conciliation step before the "Commission Nationale des Inventions de Salariés, CNIS" (i.e. the National Board for Inventions made by a Salaried Person), which has been created within the "Institut National de la Propriété Industrielle, INPI", the French Patent and Trademark Office. The CNIS has jurisdiction, *inter alia* to decide issues regarding the classification of inventions made by salaried persons, their definition, and regarding the prerogatives granted by law

(continued on next page)

law have interpreted the provisions of Article L.611-7 CIP as meaning that same apply not only to the French patent first filed to protect an invention made by a salaried person in the execution of a work contract governed by French law comprising an inventive mission corresponding to his effective functions, but also to all foreign extensions thereof, i.e. to all corresponding patent applications and/or patents filed and/or granted worldwide in order to protect said invention.

See:

- CNIS, 04.03.1981: Dossiers Brevets 1981, III, n° 5, M.P. v. Soc. S
- CNIS, 04.28.1981: Dossiers Brevets 1981, II, n° 4, M.T. v. Soc. C
- CNIS, 04.28.1981: Dossiers Brevets 1981, II, n° 3, M.J. v. Soc. P

- Court of Appeal of Paris, 4th Section, 05.10.1971: JCP ed. CI, 1972, II, 10818, Norten and Nelton v. Hureau and Générale Alimentaire ; Annales de la propriété industrielle 1973, P. 245 ; PIBD 1971, III-278 and PIBD 1972, III-42
- Court of Appeal of Paris, 4th Section, 01.22.1974: unreported, but quoted in Juris-Classeur Brevets, Fasc. 4900, n° 36
- Court of Appeal of Paris, 4th Section, 03.11.1980: PIBD 1980, III-151, Entat v. Soc. Procédés SEM and PIBD 1972, III-42, affirming District Court ("Tribunal de Grande Instance") of Paris 01.13.1978 : PIBD 1978, III-347.

III – ANALYSIS

16. As the facts disclose, Dauvois was an employee of Canal + Technologies working on information related technologies. His duty was to invent, and he did invent in

(continued from previous page)

to the employer or salaried person, in particular for disputes relating to the determination of an "additional remuneration" or a "fair price" for inventions.

./.

this technical field, all the patent applications being filed in the name of his employer, i.e.

Canal + or Canal + Technologies (see Exhibit 16).

17. In the settlement agreement executed on June 13, 2002 between Canal + Technologies and Dauvois, the latter has acknowledged expressly that :

"... in application of the article L 611-7 1°) of the CPI, [that] all the intellectual property rights to the inventions, in which Mr. Dauvois participated within the framework of the inventive missions that were entrusted to him during the years of his collaboration with the companies SECA and Canal + Technologies and particularly those that were filed and classified as an inventive mission, are the full and entire property of the Company and the remuneration stipulated in article 2.1 covers the remuneration stipulated in the said article.

Moreover, Mr. Dauvois also recognizes that in accordance with article L113-9 of the CPI, all the economic rights relating to all or part of the software applications (including their documentation), the production of which he participated in, are the exclusive property of the Company."

In addition, under the same agreement Dauvois has undertaken,

" ... to perform at the earliest possible moment or to abstain from performing all that the Company could, if necessary, ask him to perform or to abstain from performing so as to enable the Company to be able to exercise the rights or to avail themselves, irrespective of the form, of the rights that Mr. Dauvois recognises above to be the property of the Company."

See Exhibit 1 hereto.

18 In order to protect each of the Inventions Canal + Technologies filed one French and one corresponding international patent application, i.e. :

- French Application N° FR02/15978 of December 17, 2002 with the corresponding international Application N° PCT/FR2003/050181 of December 16, 2003

./.

claiming priority of FR02/15978 have been followed by US Application N° 1 covering the same invention, see Exhibits 10 and 11 paragraphs (30), (71), (72), (75);

- French Application N° FR02/04321 of April 8, 2002 with the corresponding international Application N° PCT/FR03/01024 of April 2, 2003 claiming priority of FR02/04321 have been followed by US Application N° 2 covering the same invention, see Exhibits 12 and 13 paragraphs (30), (71), (72), (75);

- French Application N° FR03/01243 of February 4, 2003 with the corresponding international Application N° PCT/EP2004/050060 of January 30, 2004 claiming priority of FR03/01343 have been followed by US Application N° 3 covering the same invention, see Exhibits 14 and 15 paragraphs (30), (71), (72), (75).

19. US patent Applications N° 1, N° 2 and N° 3 are currently standing in the name of Dauvois as Inventor / Applicant, protect the same inventions respectively as the French and corresponding international Applications identified under paragraph 18 above, and they derive therefrom.

20. Under French law which governs the employment contract between Canal + Technologies and Dauvois, all the rights on the Inventions involved are vested in Dauvois' employer, i.e. Canal + Technologies pursuant to Article L.611-7 CIP, and since with respect to each of the Inventions there is but one single invention, though protected internationally through a set of different domestic patents, according to case law the ownership rights of Canal + Technologies exist not only in France but they also extend to any and all foreign applications and/or patents covering the same invention in any country of the world.

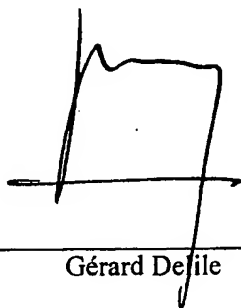
./.

21. In view of the foregoing, it is my considered opinion that in the light of the facts and the law the Inventions as well all the patent applications and/or patents protecting same worldwide belong to Canal + Technologies, including US Applications N° 1, N° 2 and N° 3, i.e. :

- Serial N° 10/538,725 filed on June 13, 2005 under the title "Method For Access Control In Digital Pay Television",
- Serial N° 10/510,533 filed on October 7, 2004 under the title "Unique Key Computation To Encipher The Data Memories",
- Serial N° 10/544,009 filed on August 1, 2005 under the title "Pay Television System, Method For Revoking Rights In Such A System, Associated Decoder and Smart Card, And Message Transmitted To Such A Decoder".

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on: February 23, 2007



Gérard Dejeu

GD/gz

CERTIFICAT DE TRAVAIL

Je soussigné, Sébastien MONTET, Responsable Ressources Humaines de la Société CANAL+ TECHNOLOGIES, certifie que :

Monsieur Jean-Luc DAUVOIS
19 rue Eugène Manuel
75016 PARIS

a été employé dans notre Société en qualité de :

- **Chef du Département Cryptologie**, au statut **Cadre**,
du **17 juillet 1995** au **06 septembre 2002**

Monsieur Jean-Luc DAUVOIS nous quitte ce jour, libre de tout engagement.

Fait à Paris, le 06 septembre 2002


Sébastien MONTET
Responsable Ressources Humaines

[CANAL+ TECHNOLOGIES letterhead]

EMPLOYMENT CERTIFICATE

I, the undersigned, Sébastien Montet, Human Resource Manager with the company CANAL
+ TECHNOLOGIES, certifies that:

Mr Jean-Luc DAUVOIS
19 rue Eugène Manuel
75016 PARIS

has been employed in our Company as:

- Chief of the Encryption department, executive status,
from July 17, 1995 to September 6, 2002

Mr Jean-Luc DAUVOIS leaves the Company as of today and is not bound by any obligation
towards the Company.

Paris, September 6, 2002

Sébastien MONTET
Human Resource Manager

PROTOCOLE TRANSACTIONNEL

ENTRE :

La Société Canal+ Technologies, société anonyme au capital de 228.899.957 francs, dont le siège social est situé 34, Place Raoul Dautry, 75516 Paris cedex 15, représentée par Monsieur Luc GERMAIN, en qualité de Directeur des Ressources Humaines France,

Ci-après désignée « *la Société* »

D'une part,

ET :

Monsieur Jean-Luc DAUVOIS, demurant 19, rue Eugène Manuel 75016 Paris.

Ci-après désigné « *M.Dauvois* »

D'autre part,

1
JLD

Article 3 Concessions de M. Dauvois

3.1 M. Dauvois convient que son contrat de travail prendra fin à la date du 6 septembre 2002, date d'expiration de son préavis.

Au regard des concessions effectuées par la Société, M. Dauvois accepte de ne pas donner suite à ses contestations, tant sur le fond que sur la procédure ayant conduit à son licenciement.

M. Dauvois reconnaît que les concessions faites par l'employeur sont réalisées à titre transactionnel, forfaitaire et définitif, conformément aux dispositions des articles 2044 et suivants du Code Civil, et en particulier de l'article 2052 dudit Code, ceci afin de le remplir de tous ses droits et pour mettre fin à tout différend né ou à naître des rapports de droit ou de fait ayant pu exister entre la Société et les Sociétés du Groupe Canal+ d'une part et M. Dauvois d'autre part.

3.2 M. Dauvois reconnaît, en tant que de besoin, qu'en application de l'article L 611-7 1°) du CPI, l'intégralité des droits de propriété intellectuelle sur les inventions auxquelles M. Dauvois a participé dans le cadre des missions inventives qui lui ont été confiées pendant les années de sa collaboration avec les sociétés SECA et Canal+ Technologies et notamment celles qui ont fait l'objet d'un dépôt valant classement en invention de mission, sont la propriété pleine et entière de la Société et que la rémunération stipulée à l'article 2.1 couvre la rémunération prévue audit article.

4
JLD

M. Dauvois reconnaît, en outre, que conformément à l'article L 113-9 du CPI l'ensemble des droits patrimoniaux relatifs à tout ou partie des logiciels (en ce compris leur documentation) à l'élaboration desquels il a été amené à participer sont la propriété exclusive de la Société.

M. Dauvois s'engage à faire dans les meilleurs délais ou à s'abstenir de faire tout ce que la Société pourrait, le cas échéant, lui demander de faire ou de s'abstenir de faire afin de permettre à la Société de pouvoir exercer les droits ou de se prévaloir, de quelque façon que ce soit, des droits que M. Dauvois reconnaît ci-dessus être la propriété de la Société.

Enfin M. Dauvois s'engage à fournir tous les éléments nécessaires au dépôt des brevets suivants :

- I2000-022
- I2001-015
- I2001-022
- I2002-011 (Fiche d'invention « notoirement » incomplète)
- I2002-012 (Fiche d'invention « notoirement » incomplète)
- I2002-013 (Fiche d'invention « notoirement » incomplète)
- I2002-014 (Fiche d'invention « notoirement » incomplète)
- I2002-015 (Fiche d'invention « notoirement » incomplète)
- I2002-016 (Fiche d'invention « notoirement » incomplète)
- I2002-017 (Fiche d'invention « notoirement » incomplète)
- I2002-018 (Fiche d'invention « notoirement » incomplète)

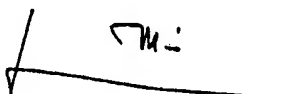
En outre, il s'engage à signer les documents d'extension et reconnaît que ces brevets sont la propriété pleine et entière de la Société et que la rémunération stipulée à l'article 2.1 couvre la rémunération prévue audit article.

4
JLD

8. déclarent que le présent Accord aura, entre les parties, le même effet juridique qu'une décision judiciaire passée en force de chose jugée.

Fait en deux originaux à Paris, le 12 juin 2002

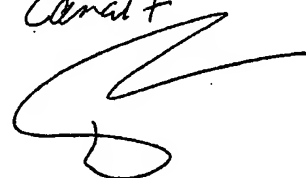
Lu et approuvé
Bon pour Transaction
irrévocable et
désistement de tous droits,
instances et actions



Pour la Société Canal+ Technologies
Luc Germain

(Faire précéder la signature de la mention manuscrite :
« Lu et approuvé. Bon pour transaction irrévocable et
désistement de tous droits, instances et actions »)

Lu et approuvé. Bon pour
Transaction irrévocable et désistement
de tous droits instances et actions. Bon
pour quittance des sommes visées dans
le corps des présentes. Bon pour
renonciation à tout recours contre la
Société et toute autre société
du Groupe Canal+



Jean-Luc Dauvois

(Faire précéder la signature de la mention manuscrite :
« Lu et approuvé. Bon pour transaction irrévocable et
désistement de tous droits, instances et actions. Bon
pour quittance des sommes visées dans le corps des
présentes. Bon pour renonciation à tout recours contre
la Société et toute autre société du Groupe Canal+ »)

COMPROMISE AGREEMENT

BETWEEN:

Canal+ Technologies, public limited company with a share capital of 228,899,957 Francs,
whose registered office is located at 34, Place Raoul Dautry, 75516 Paris Cedex,
represented by Mr. Luc Germain, acting as Director of Human Resources France,

Hereafter called *"the Company"*

On the one hand,

AND:

Mr. Jean-Luc Dauvois, residing at 19, rue Eugène Manuel 75016 Paris.

Hereafter called *"Mr. Dauvois"*

On the other,

Article 3 Concessions of Mr. Dauvois

3.1 Mr. Dauvois agrees that his employment contract will terminate on the date of 6 September 2002, date that his period of notice expires.

With regard to the concessions made by the Company, Mr. Dauvois accepts not to pursue his differences concerning both the substance and procedure having lead to his dismissal.

Mr. Dauvois recognises that the concessions made by the employer were performed as a fixed, definitive compromise in accordance with the provisions of articles 2044 and above of the French Civil Code, and in particular article 2052 of the said Code, in order to fulfil all his rights and to end any difference that has arisen or will arise from the legal or de facto relations that may have existed between the Company and the Companies of the Canal+ group on the one hand and Mr. Dauvois on the other.

3.2 Mr. Dauvois recognises, where necessary, in application of the article L 611-7 1°) of the CPI, that all the intellectual property rights to the inventions, in which Mr. Dauvois participated within the framework of the inventive missions that were entrusted to him during the years of his collaboration with the companies SECA and Canal+ technologies and particularly those that were filed and classified as an inventive mission, are the full and entire property of the Company and that the remuneration stipulated in article 2.1 covers the remuneration stipulated in the said article.

Moreover, Mr. Dauvois also recognises that in accordance with article L113-9 of the CPI, all the economic rights relating to all or part of the software applications (including their documentation), the production of which he participated in, are the exclusive property of the Company.

Mr. Dauvois agrees to perform at the earliest possible moment or to abstain from performing all that the Company could, if necessary, ask him to perform or to abstain from performing so as to enable the Company to be able to exercise the rights or to avail themselves, irrespective of the form, of the rights that Mr. Dauvois recognises above to be the property of the Company.

Finally, Mr. Dauvois agrees to supply all the elements necessary to file the following patents:

- 12000-022
- 12001-015
- 12001-022
- 12001-011 (invention sheet "notably" incomplete)
- 12001-012 (invention sheet "notably" incomplete)
- 12001-013 (invention sheet "notably" incomplete)
- 12001-014 (invention sheet "notably" incomplete)
- 12001-015 (invention sheet "notably" incomplete)
- 12001-016 (invention sheet "notably" incomplete)
- 12001-017 (invention sheet "notably" incomplete)
- 12001-018 (invention sheet "notably" incomplete)

Moreover, he undertakes to sign the extension documents and recognises that these patents are the full and entire property of the Company and that the remuneration stipulated in article 2.1 covers the remuneration provided for in the said article.

8. declare that the present agreement will have the same legal force between the parties as a judgment having force of *res judicata*.

Signed in two original copies at Paris, on 13 June 2002

Handwritten wording:
Read and approved. Good for
irrevocable transaction and
withdrawal of all rights, suits and
actions
Handwritten signature

For Canal+ Technologies
Luc Germain

(Precede the signature with the
following handwritten wording:
"Read and approved. Good for
irrevocable transaction and withdrawal
of all rights, suits and actions")

Handwritten wording:
Read and approved. Good for irrevocable
transaction and withdrawal of all rights, suits
and actions. Good for acknowledgement of
receipt of the amounts specified in the body
of this agreement. Good for renunciation of
any recourse against the Company or any
other company of the Canal+ group
Handwritten signature

Jean-Luc Dauvois

(Precede the signature with the
following handwritten wording:
"Read and approved. Good for
irrevocable transaction and withdrawal
of all rights, suits and actions. Good for
acknowledgement of receipt of the
amounts specified in the body of this
agreement. Good for renunciation of
any recourse against the Company or
any other company of the Canal+
group")

Système d'insertion dans le cadre
Date de réception : 01/05/2006
Données saisies :
Référence : 120001016

DECLARATION D'INVENTION

Veillez remplir et cocher les champs, imprimer puis signer et renvoyer à : Bruno Weihs.
Envoyez également le fichier Word.

1. Titre de l'invention : Unique Key Computation To Enciphered The Data Memories

Inventeur 1 (rédacteur de la déclaration) :

Nom : DAUVOIS Jean-Luc

Employé Canal+ Technologies : ☒

Prestataire : ☐

Inventeur 2

Nom :

Employé Canal+ Technologies : ☐

Prestataire : ☐

Inventeur 3

Nom :

Employé Canal+ Technologies : ☐

Prestataire : ☐

Autres inventeurs en annexe ☐

2. L'invention a déjà été divulguée ? non

Si oui, existait-il un accord de confidentialité ? ...

Si non, quand est-il prévu de divulguer l'invention ?

Date :

A qui ?

3. Domaine Technique de l'invention : Hardware pour carte à puce
Projet éventuel :

4. Classement de l'invention :

De mission : ☒

Hors mission : ☐

5. Recherche d'art antérieur souhaité ? oui

Si oui, donner des mots clés :
Encryption by a Unique Key

Les paragraphes suivants sont destinés à situer et décrire l'invention. Les informations fournies pourront servir à la préparation d'une demande de brevet. Le texte peut être en français ou en anglais. Il serait dans la majorité des inventions utile de fournir des figures pour illustrer le texte.

6. Art antérieur - Problème

Décrire le contexte dans lequel l'invention a été faite (sans décrire l'invention) en mentionnant l'art antérieur connu de vous ainsi que le(s) problème(s) qui se pose(nt) et qui devra être résolu par l'invention. Décrire également les solutions connues au problème.

Figure(s) en annexe : ☐ oui

Numéros des figures :

Le piratage par carte à puce prend en général la forme d'une extraction du Rom code et des mémoires associées contenant en général les données sensibles (les clés). Pour éviter que ces données sensibles soient directement utilisables il est nécessaire de les chiffrer avant de les stocker en mémoire. Cependant qui dit chiffrement dit clé et donc stockage de la (ou les) clés de chiffrement. Pour éviter de stocker directement la clé (qui doit être unique par composant) en mémoire il peut être intéressant de la recalculer à chaque fois (chaque reset). Cette clé devra cependant faire appel à une fonction propre du composant (et immuable avec les conditions d'environnement et le temps). Pour cela deux possibilités: soit utiliser directement ce que le chip nous propose avec le temps de mise ne charge de la tension d'alimentation de l'EEPROM, soit d'ajouter une fonction logique sur le chip si c'est possible pour faire directement un calcul de la clé de chiffrement.

7. Résumé

Résumer l'idée générale de l'invention.

Figure(s) en annexe : ☐ oui

Numéros des figures :

A chaque Reset le CPU ira calculer la clé de chiffrement des autres clés. pour cela il prendra par exemple en compte la mesure du temps de mise en charge de la tension de l'EEPROM (immuable). Ainsi si un hacker extrait les codes et données il ne pourra pas recalculer les clés puisqu'il ne disposera pas des paramètres physique du chip. les hackers n'auront donc aucun avantages à extraire les données des mémoires. Cette clé unique mise en place pour la première fois lors de la personnalisation par exemple.

8. Solutions – Avantages

En quoi l'invention résout-elle le problème ?

Quel(s) avantage(s) apporte l'invention par rapport à l'art antérieur ?

Permet de lier de façon très étroites le software, les données (clés) et le hardware du composant.

9. Description détaillée

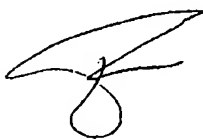
Description détaillée de l'invention comprenant au moins un exemple de réalisation de l'invention.

Figure(s) en annexe : ☐ oui

Numéros des figures :

voir résumé

Signature(s)



Inventeur 1 :

Date :

Inventeur 2 :

Date :

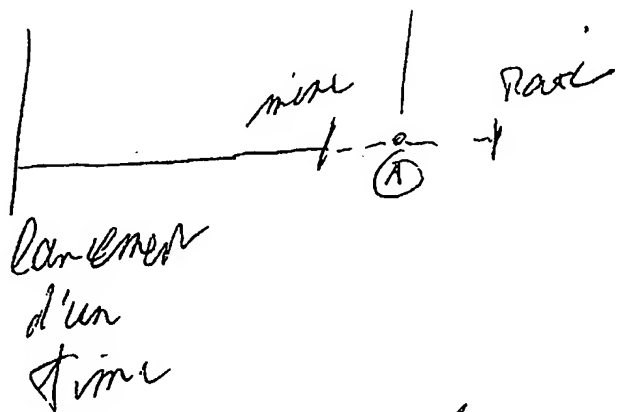
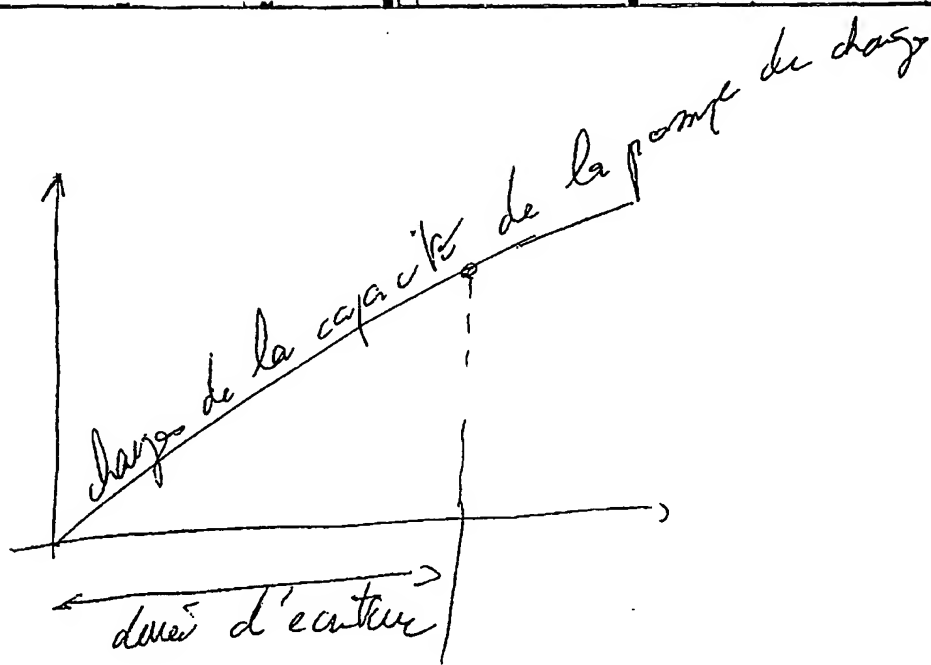
Inventeur 3 :

Date :

ANNEXE

Autres inventeurs :

Nom :	Employé Canal+ Technologies : <input type="checkbox"/>
	Prestataire : <input type="checkbox"/>
Nom :	Employé Canal+ Technologies : <input type="checkbox"/>
	Prestataire : <input type="checkbox"/>
Nom :	Employé Canal+ Technologies : <input type="checkbox"/>
	Prestataire : <input type="checkbox"/>
Nom :	Employé Canal+ Technologies : <input type="checkbox"/>
	Prestataire : <input type="checkbox"/>
Nom :	Employé Canal+ Technologies : <input type="checkbox"/>
	Prestataire : <input type="checkbox"/>
Nom :	Employé Canal+ Technologies : <input type="checkbox"/>
	Prestataire : <input type="checkbox"/>



* Le Timer nous donne la valeur de la cb (on aura plus soin de filtrer la valeur \textcircled{A} pour être sûr de calculer la bonne cb -

* on pourrait faire la même chose avec les mesures de seuils de déclenchement des sensors de température et de tension

ANAL+
TECHNOLOGIES

34 PLACE RAOUL DAUTRY 75906 PARIS CEDEX 15 FRANCE
TEL 33 1 71 71 57 15

Bruno Weihs
Département Juridique et Propriété Intellectuelle
Tel: 01 71 71 55 82
Fax: 01 71 71 52 02
Email bweihs@canal-plus.fr

BREVALEX
Monsieur Guy Dubois-Chabert
3 rue du Docteur Lancereaux
75008 PARIS

Paris, le 26 juin 2001

Par télécopie et confirmation courrier
Confidentiel

N/Réf: 12001.016
BW/NH/01.365

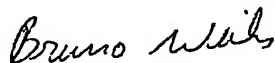
Objet: Déclaration d'invention
Titre: «Unique Key Computation to enciphered the data memories »
Inventeur: Jean-Luc Dauvois

Monsieur,

J'ai l'honneur de vous faire parvenir par la présente une nouvelle déclaration d'invention contenant une description d'invention que nous souhaiterions protéger avec un brevet français.

Je propose qu'une réunion ait lieu entre un ingénieur de votre société et l'inventeur afin de compléter la déclaration d'invention, d'effectuer une éventuelle recherche d'antériorités et de préparer un projet de rédaction d'une demande de brevet.

Je vous prie d'agréer, Monsieur, l'expression de mes salutations les plus sincères.



Bruno WEIHS

P.J. : Déclaration d'invention

c.c.(sans P.J.): Jean-Luc Dauvois



MEMORANDUM

Réf : I 2001.016
BA/NH/01.481

Date : 5 novembre 2001

De/From : Bertrand ALLAIN

A/To : Jean-Luc DAUVOIS

Objet : Nouvelle demande de brevet
Titre : « Procédé et dispositif de protection de données numériques
stockées dans une mémoire »

Jean-Luc,

J'ai le plaisir de te faire parvenir par la présente un projet de demande de brevet préparé par Brevaux, pour relecture.

Il est important que tu vérifies l'exactitude et la portée de la description, ainsi que le contenu des revendications par rapport à l'invention.

Tu pourras me retourner le document annoté avec tes remarques et/ou corrections et le cas échéant avec la mention « Bon pour dépôt » et ta signature sur la première page des revendications.

Cordialement,

P/0 
Bertrand ALLAIN

P.J. : Projet de demande de brevet

CONFIDENTIEL

ANAL+
TECHNOLOGIES

34 PLACE RAOUL DAUTRY 75906 PARIS CEDEX 15 FRANCE
TEL 33 1 71 71 57 15

Bertrand Allain
Directeur Juridique et de la Propriété Intellectuelle
Tel: 01 71 71 57 59
Fax: 01 71 71 52 02
Email ballain@canal-plus.fr

BREVALEX
Monsieur Houssine Moudni
3 rue du Docteur Lancereaux
75008 PARIS

Paris, le 12 novembre 2001

V/Réf: 20022/HM
N/Réf: I2001.016
BA/NH/01.488

Objet: Projet de demande de brevet français
Titre: «Procédé et dispositif de protection de données numériques stockées dans une mémoire »
Inventeur: Jean-Luc Dauvois

Cher Monsieur,

Je vous prie de trouver ci-joint le texte que vous nous aviez fait parvenir concernant le projet référencé en objet.

Le projet est annoté par Jean-Luc Dauvois. Je propose que vous considériez les suggestions de modifications et que vous contactiez l'inventeur au cas où vous auriez des questions.

Je vous prie d'agréer, Cher Monsieur, l'expression de mes sentiments distingués.


Bertrand ALLAIN

P.J. : Projet annoté

Paris, le 31 octobre 2001

SP 20022/HM

V.réf : I2001.016

PROJET DE DEMANDE DE BREVET FRANCAIS

TITRE

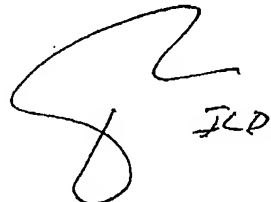
PROCEDE ET DISPOSITIF DE PROTECTION DE DONNEES
NUMERIQUES STOCKEES DANS UNE MEMOIRE

ooo

CANAL + TECHNOLOGIES

ooo

- 1) Faire apparaître visiblement les modifications souhaitées
- 2) RAYER les lignes ou paragraphes à supprimer

Voir les Modifications / corrections
à l'intérieur
le 11/10/01  JLD

SP 20022/HM

U

PROCÉDE ET DISPOSITIF DE PROTECTION DE DONNEES
NUMERIQUES STOCKEES DANS UNE MEMOIRE

Domaine technique

5 L'invention se situe dans le domaine de la
lutte contre le piratage du contenu des mémoires de
stockage de données et concerne plus particulièrement
un procédé de protection de données numériques cryptées
par une clé de chiffrement et ~~stockées dans une~~
✓ ~~mémoire.~~

10 L'invention concerne également une carte à puce
et un dispositif de protection de la mémoire de cette
carte à puce.

Etat de la technique antérieure

15 Le piratage d'une carte à puce se fait en
général par l'extraction du code ROM et des mémoires
associées contenant des données secrètes. Une technique
connue pour éviter que ces données sensibles ne soient
utilisables après une extraction frauduleuse consiste à
20 les chiffrer au moyen de clés secrètes avant de les
stocker dans la mémoire de la carte. Les clés de
chiffrement utilisées sont également stockées dans une
mémoire de la carte. Le fait de mémoriser les clés de
chiffrement dans la mémoire de la carte à puce expose
25 ces dernières à une extraction frauduleuse au même
titre que les données utiles mémorisées. Aussi, cette
technique ne permet-elle pas de lutter efficacement
contre le piratage.

30 Le but de l'invention est d'assurer une
sécurité optimale des données mémorisées sous forme
cryptée dans une mémoire.

Un autre but de l'invention est de lier intimement les clés de chiffrement à un ou plusieurs paramètres de fonctionnement intrinsèque à cette mémoire. Ces paramètres de fonctionnement pouvant être
 5 des grandeurs physiques dépendant de la structure physique de la mémoire ou encore des grandeurs reflétant un comportement déterminé de cette mémoire dans des conditions particulières d'utilisation.

2 ou encore de grandeurs reflétant un comportement déterminé de mino. contrôleur associé à cette mémoire

10 Exposé de l'invention

De façon plus précise, l'invention concerne un procédé et un dispositif de protection de données numériques stockées sous forme cryptée dans une mémoire qui peut être du type EEPROM ou du type flash par
 15 exemple.

Le procédé selon l'invention est caractérisé par le fait que ladite clé de chiffrement est définie dynamiquement en fonction d'au moins un paramètre de fonctionnement intrinsèque à ladite mémoire.

20 Préférentiellement, le procédé comporte les étapes suivantes :

• lors de la phase d'écriture des données dans la mémoire,

a- dériver un signal analogique d'une tension
 25 analogique d'écriture dans la mémoire,

b- convertir ce signal en une séquence numérique,

c- chiffrer les données à mémoriser au moyen de ladite séquence numérique,

30 d- stocker les données chiffrées dans la mémoire,

•et lors d'une phase ultérieure de lecture des données mémorisées,

- recalculer la clé de chiffrement définie aux étapes a et b de la phase d'écriture et

5 - décrypter les données au moyen de la clé recalculée.

Dans une application particulière du procédé, la mémoire est agencée sur une carte de contrôle d'accès.

10 Selon un mode de réalisation, la tension analogique d'écriture est fournie par une pompe de charge.

Le dispositif selon l'invention est caractérisé par le fait qu'il comporte un module de calcul apte à
15 définir une clé de chiffrement des données numériques à mémoriser en fonction d'au moins un paramètre de fonctionnement intrinsèque à ladite mémoire, et par le fait que ledit module de calcul recalcule dynamiquement ladite clé de chiffrement à chaque lecture des données
20 mémorisées.

Selon un mode de réalisation de l'invention, le module de calcul extrait un signal analogique d'une tension analogique d'écriture délivrée par une pompe de charge et convertit ce signal analogique en une
25 séquence numérique pour constituer la clé de chiffrement.

L'invention concerne également une carte de contrôle d'accès comportant une unité centrale de traitement de données, au moins une mémoire de stockage
30 de données, un module de chiffrement desdites données

numériques et un module de calcul d'au moins une clé de chiffrement desdites données.

La carte de contrôle d'accès selon l'invention comporte des moyens pour définir la clé de chiffrement en fonction d'au moins un paramètre de fonctionnement intrinsèque à la mémoire de ladite carte, et des moyens pour recalculer dynamiquement la clé de chiffrement préalablement définie à chaque lecture des données mémorisées.

10 Selon une caractéristique de l'invention le module de calcul est fonctionnellement indépendant de l'unité centrale de sorte que le calcul de la clé de chiffrement n'est pas supervisé par l'unité centrale de traitement. *mais juste initio*

15 Selon un mode particulier de réalisation de l'invention, le module de calcul comporte une pompe de charge destinée à fournir une tension analogique d'écriture des données dans la carte à puce, un convertisseur analogique/numérique destiné à convertir
20 un signal analogique extrait de ladite tension analogique en une séquence numérique constituant la clé de chiffrement.

Brève description des dessins

25 D'autres caractéristiques et avantages de l'invention ressortiront de la description qui va suivre, prise à titre d'exemple non limitatif, en référence aux figures annexées, dans lesquelles :

- la figure 1 représente un schéma général d'un
30 dispositif selon l'invention.

- la figure 2 représente schématiquement un mode particulier de réalisation du dispositif de la figure 1.

- la figure 3 représente une courbe illustrant une mise en œuvre de l'invention dans le cas de l'exemple illustré par la figure 2.

Exposé détaillé de modes de réalisation particuliers

L'invention va maintenant être décrite dans le cadre de la protection des données stockées dans la mémoire d'une carte à puce.

Les cartes à puces ~~appelées également cartes à mémoire~~ sont largement utilisées notamment pour mémoriser des paramètres de contrôle d'accès à des données ou services tels que par exemple des programmes audiovisuels cryptés. Dans ce type d'application, les informations nécessaires au désembrouillage sont transmises dans des messages de contrôle d'accès ~~spécifiques appelés messages d'accès conditionnel~~ (Conditional Access Messages - CAM), qui sont de deux types ECM (Entitlement Control Message) et EMM (Entitlement Management Message) et sont générés à partir de trois données d'entrées :

- un mot de contrôle (Control Word) destiné à initialiser la séquence de désembrouillage,

- une clé de service (Service Key) utilisée pour embrouiller le mot de contrôle, pour un groupe d'un ou de plusieurs utilisateurs,

- une clé utilisateur (user key) utilisée pour embrouiller la clé de service.

5
notamment

Les ECM sont ~~de~~ fonction du mot de contrôle et de la clé de service et sont transmis aux abonnés à intervalles réguliers (~~toutes les deux secondes environ~~).

5 Les EMM sont *notamment* fonction de la clé de service et de la clé utilisateur, et sont également transmis aux abonnés à intervalles réguliers (~~toutes les dix secondes environ~~).

10 A la réception, le principe de décryptage consiste à retrouver la clé de service à partir de la clé utilisateur contenue dans la mémoire d'une carte à puce. Cette clé de service est ensuite elle-même utilisée pour décrypter les ECM afin de retrouver le mot de contrôle permettant l'initialisation du système
15 de désembrouillage.

Comme cela a été expliqué précédemment, le contenu de la mémoire de la carte à puce peut être extrait et réutilisé de façon frauduleuse pour retrouver les EMM et les ECM nécessaires au calcul du
20 mot de contrôle permettant l'initialisation du système de désembrouillage.

La figure 1 représente un schéma bloc général d'un dispositif à mémoire comportant une unité centrale de traitement 2 reliée à une mémoire 4 via un module de
25 cryptage/décryptage 6. Un module de calcul 10, agencé extérieurement à l'unité centrale 2, est également relié au module de cryptage/décryptage 6.

Lorsque des données traitées dans l'unité centrale 2 doivent être stockées dans la mémoire 4,
30 l'unité de traitement 2 envoie au module de calcul ¹⁰ ② un signal d'activation. A la réception de ce signal, le

??

module de calcul (2) définit une clé de chiffrement des données à mémoriser et transmet cette clé au module de cryptage/décryptage 6.

Selon une caractéristique essentielle de l'invention, la clé de chiffrement est calculée au moment de la mémorisation des données dans la mémoire 4 en fonction d'au moins un paramètre de fonctionnement intrinsèque à la mémoire 4. La clé de chiffrement ainsi calculée n'est pas stockée dans la mémoire 4. Or le piratage des cartes à puces consiste généralement à extraire les programmes de calcul mis en œuvre dans l'unité centrale 2 et les données sensibles contenues dans la mémoire 4 associée à l'unité centrale 2. Aussi, en cas d'extraction frauduleuse de ces programmes et du contenu de la mémoire 4, les données extraites seront inutilisables sans la clé de chiffrement qui est calculée dynamiquement lors de la mémorisation desdites données et lors de la lecture de ces données.

Préférentiellement, cette clé est calculée en fonction d'un paramètre ou d'une combinaison de plusieurs paramètres de fonctionnement intrinsèque à ladite mémoire 4.

La clé de chiffrement définie est inaccessible de l'extérieur, du fait que le module de calcul 10 est indépendant de l'unité centrale 2.

En fonctionnement, au moment du transfert des données de l'unité centrale 2 vers le module de calcul 10, ce dernier reçoit de l'unité centrale 2 un premier signal d'activation, lui permettant de commencer le calcul de la clé de chiffrement. La clé ainsi calculée est transmise au module de cryptage/décryptage 6 qui

l'utilise pour chiffrer les données avant que ces dernières ne soient mémorisées dans la mémoire 4.

Lorsque les données cryptées doivent être lues, l'unité de traitement 2 envoie au module de calcul 10 un deuxième signal d'activation pour recalculer dynamiquement la clé de chiffrement qui est ensuite utilisée par le module de cryptage/décryptage 6 pour décrypter lesdites données et les transmettre à l'unité centrale 2.

Un exemple particulier de calcul de la clé de chiffrement va être décrit maintenant en référence à la figure 2 représentant un exemple de réalisation de l'invention dans lequel le module 10 est constitué par la pompe de charge 12 destinée à fournir une tension analogique d'écriture des données dans la mémoire 4, un convertisseur analogique-numérique (CAN) 14 destiné à convertir un signal analogique extrait de ladite tension analogique en une séquence numérique constituant la clé de chiffrement, une horloge 16 reliée à la pompe de charge 12 destinée à fixer la durée du signal analogique extrait de la tension d'écriture.

La figure 3 représente schématiquement l'évolution en fonction du temps de la tension d'écriture 18 des données numériques provenant de l'unité centrale 2 dans la mémoire 4. Une valeur A de la tension 18 est fixée par programmation de la durée t au moyen de l'horloge 16. Cette valeur A est ensuite convertie par le CAN 14 en une séquence numérique S qui est utilisée par le module de cryptage/décryptage 6 pour crypter/décrypter les données numériques.

A chaque remise à zéro, le module de calcul 10 calcule la clé de chiffrement en prenant en considération la durée t programmée au moyen de l'horloge 16. Ainsi, si un pirate extrait les données 5 numériques ~~et les charge dans une carte falsifiée~~, il ne pourra pas recalculer la clé de chiffrement qui dépend de la valeur A qui est intrinsèque à la carte authentique. La clé de chiffrement est calculée pour la première fois lors de la personnalisation de la carte à 10 puce.

Dans une variante de réalisation de l'invention, plusieurs durées t correspondant à plusieurs valeurs A peuvent être préprogrammées afin d'être utilisées successivement pour calculer plusieurs 15 clés de chiffrement différentes, chaque clé pouvant être utilisée pendant une période prédéfinie.

Dans une autre variante de réalisation, la durée t peut être modifiée à distance.

20

~~pour ainsi~~
 une autre variante, la pompe
 de dosage peut être remplacée
~~aisément~~
 aisément par une fonction
 analogique ou numérique

REVENDICATIONS

1. Procédé de protection de données numériques cryptées par une clé de chiffrement et stockées dans une mémoire (4), caractérisé en ce que ladite clé de chiffrement est définie dynamiquement en fonction d'au moins un paramètre de fonctionnement intrinsèque ~~à ladite mémoire (4).~~ *au micro-contrôleur carte à puce*
2. Procédé selon la revendication 1, caractérisé en ce qu'il comporte les étapes suivantes :
- lors de la phase d'écriture des données dans la mémoire (4),
 - a- dériver un signal analogique d'une tension analogique (18) d'écriture dans la mémoire (4),
 - b- convertir ce signal en une séquence numérique S,
 - c- chiffrer les données à mémoriser au moyen de ladite séquence numérique S,
 - d- stocker les données chiffrées dans la mémoire (4).
 - et lors d'une phase ultérieure de lecture des données mémorisées,
 - recalculer la clé de chiffrement définie aux étapes a et b, et
 - décrypter les données au moyen de la clé recalculée.
3. Procédé selon la revendication 2, caractérisé en ce que ladite mémoire (4) est agencée sur une carte à puce de contrôle d'accès.

4. Procédé selon la revendication 3, caractérisé en ce que la tension analogique d'écriture (18) est fournie par une pompe de charge (12).

5

5. Dispositif de protection de données numériques cryptées par une clé de chiffrement et stockées dans une mémoire (4), caractérisé en ce qu'il comporte un module de calcul (10) apte à définir la clé de chiffrement desdites données en fonction d'au moins un paramètre de fonctionnement intrinsèque à ladite mémoire (4), et en ce que ledit module de calcul (10) recalcule dynamiquement ladite clé de chiffrement à chaque lecture des données mémorisées.

15 *remise sous tension, ou à tout moment opportun*

6. Dispositif selon la revendication 5, caractérisé en ce que ladite clé de chiffrement est calculée à partir d'une tension analogique (18) d'écriture des données dans la mémoire de la carte à puce.

20

7. Dispositif selon la revendication 6, caractérisé en ce que ladite mémoire est agencée sur une carte de contrôle d'accès.

25

8. Dispositif selon la revendication 7, caractérisé en ce que ladite tension analogique d'écriture est délivrée par une pompe de charge.

30 9. Dispositif selon la revendication 6, caractérisé en ce que le module de calcul (10) extrait

un signal analogique de ladite tension (18) et convertit ce signal analogique en une séquence numérique pour constituer la clé de chiffrement.

5 10. Dispositif selon la revendication 9, caractérisé en ce que le module de calcul (10) comporte un convertisseur analogique/numérique (14).

10 11. Carte de contrôle d'accès comportant une unité centrale de traitement de données, au moins une mémoire de stockage de données, un module de chiffrement (6) desdites données numériques et un module de calcul (10) d'au moins une clé de chiffrement desdites données, caractérisée en ce que ledit module
15 de calcul (10) comporte des moyens pour définir la clé de chiffrement en fonction d'au moins un paramètre de fonctionnement intrinsèque à ladite mémoire (4), et des moyens pour recalculer dynamiquement ladite clé de chiffrement à chaque lecture des données mémorisées.

20 12. Carte de contrôle d'accès selon la revendication 11, caractérisée en ce que le module de calcul (10) est fonctionnellement indépendant de l'unité centrale (2) de sorte que le calcul de la clé
25 de chiffrement n'est pas supervisé par l'unité centrale de traitement (2).

30 13. Carte à puce selon la revendication 12, caractérisée en ce que le module de calcul (10) comporte une pompe de charge (12) destinée à fournir une tension analogique (18) d'écriture des données dans

la carte à puce, un convertisseur analogique-numérique (14) destiné à convertir un signal analogique extrait de ladite tension analogique (18) en une séquence numérique S constituant la clé de chiffrement,

5

14. Carte à puce selon la revendication 11, caractérisée en ce que le module de chiffrement (6) est un circuit logique.

10

15. Carte à puce selon l'une des revendications 11 à 14, caractérisée en ce que la mémoire (4) est du type EEPROM.

15 16. Carte à puce selon l'une des revendications 11 à 14, caractérisée en ce que la mémoire (4) est du type flash.

à faire une description indiquant
que la fonction 10 est une
fonction analogique (indépendante
de la pompe de charge)

à faire une description indiquant
que la fonction 10 est une fonction
numérique

[Note: la pompe de charge ne doit être
qu'un exemple de réalisation —
SP 20Q22/HM

ABRÉGÉ DESCRIPTIF

5 L'invention concerne un procédé de protection de données numériques cryptées par une clé de chiffrement et stockées dans une mémoire (4).

10 Le procédé selon l'invention est caractérisé par le fait que ladite clé de chiffrement est définie dynamiquement en fonction d'au moins un paramètre de fonctionnement intrinsèque à ladite mémoire.

Fig 1

1/2

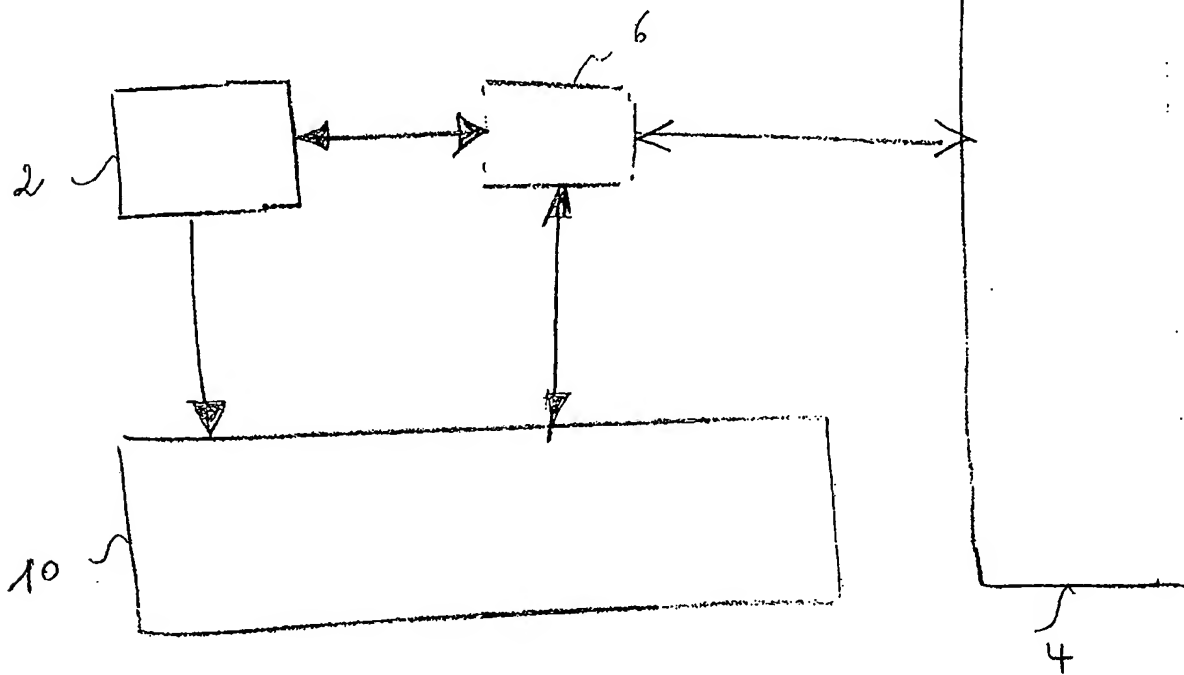


FIG 1

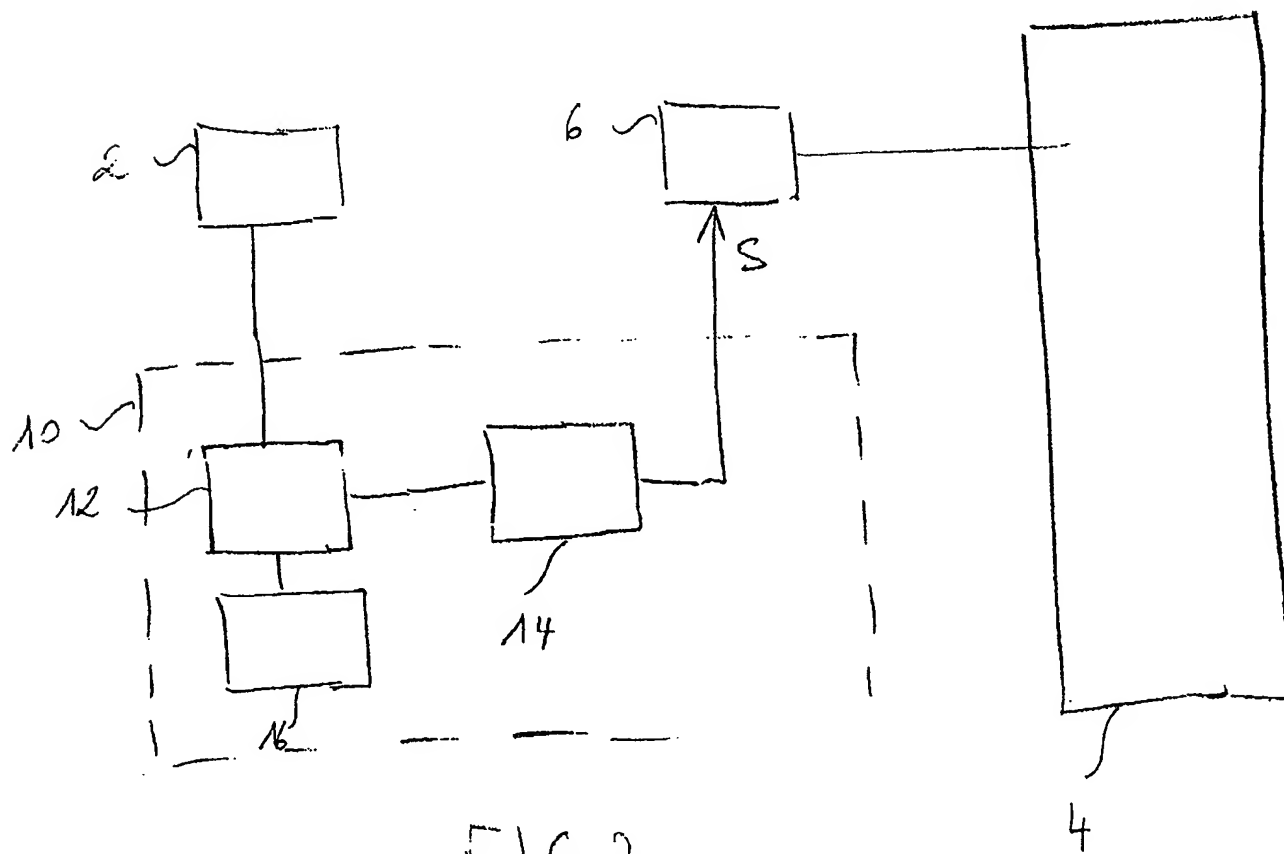


FIG 2

2/2

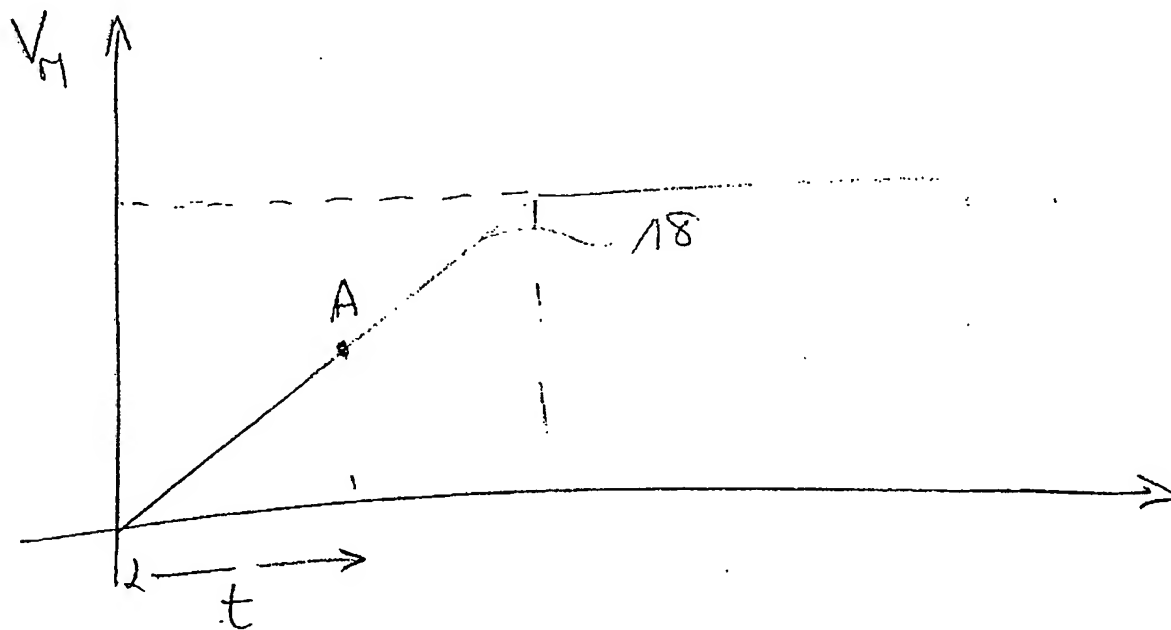
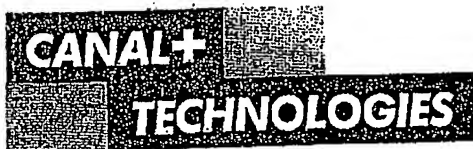


FIG 3



MEMORANDUM

Réf : B 2002.005
PC/NH/02.152

Date : 16 avril 2002

De/From : Philippe CASSAGNE

A/To : Sébastien MONTET

Objet : Nouvelle demande de brevet européen
Titre : « Procédé et dispositif de protection de données numériques
stockées dans une mémoire »
Inventeur: Jean Luc Dauvois

Sébastien,

Selon la nouvelle procédure concernant les primes d'invention, je te prie de noter que [REDACTED] a été désigné en tant qu'inventeur pour la demande de brevet français intitulée « Procédé et dispositif de protection de données numériques stockées dans une mémoire ». Cette demande est une première demande dans la famille brevets. Elle a été déposée auprès de l'INPI le 8 avril 2002 et a obtenu le numéro de dépôt 02 04321.

Conformément à ce qui a été convenu, l'inventeur devra obtenir dans les meilleurs délais, une prime d'invention d'un montant de 5000,00 FF.

Je reste à ta disposition pour toute information complémentaire.

Cordialement,

BON POUR ACCORD

Philippe CASSAGNE

Date

Signature

SEBASTIEN MONTET

Date

Signature

CONFIDENTIEL



34 PLACE RAOUL DAUTRY 75906 PARIS CEDEX 15 FRANCE
TEL 33 1 71 71 57 15

Monsieur Jean-Luc DAUVOIS

Paris, le 23 avril 2002

Monsieur,

J'ai le plaisir de vous annoncer, suite à votre participation en tant qu'inventeur dans la demande de brevet français intitulé "**Procédé et dispositif de protection de données numériques stockées dans une mémoire**", déposée le 8 avril 2002 (réf de dépôt INPI 02 04321) qu'il vous est attribué une prime d'un montant brut forfaitaire de :

762,25 euros

Cette somme sera versée avec vos appointements du mois de mai 2002.

Je vous prie d'agréer, Monsieur, l'expression de ma considération distinguée

Philippe DURANTON
Directeur Général Adjoint,
Affaires Générales et Ressources Humaines

A handwritten signature in black ink, appearing to read "Philippe Durantont", written over a horizontal line.

①9 RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
PARIS

①1 N° de publication :
(à n'utiliser que pour les
commandes de reproduction)

2 848 764

②1 N° d'enregistrement national :

02 15978

⑤1 Int Cl⁷ : H 04 N 7/167

⑫

DEMANDE DE BREVET D'INVENTION

A1

②2 Date de dépôt : 17.12.02.

③0 Priorité :

④3 Date de mise à la disposition du public de la
demande : 18.08.04 Bulletin 04/25.

⑤6 Liste des documents cités dans le rapport de
recherche préliminaire : *Se reporter à la fin du
présent fascicule*

⑥0 Références à d'autres documents nationaux
apparentés :

⑦1 Demandeur(s) : CANAL + TECHNOLOGIES Société
anonyme — FR.

⑦2 Inventeur(s) : DAUVOIS JEAN LUC.

⑦3 Titulaire(s) :

⑦4 Mandataire(s) : THOMSON.

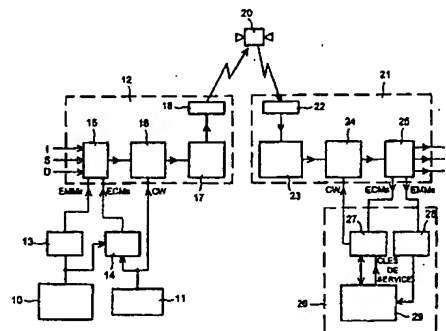
⑤4 PROCÉDE DE CONTRÔLE D'ACCES EN TELEVISION NUMERIQUE PAYANTE.

⑤7 L'invention concerne un procédé de contrôle d'accès,
en télévision numérique payante, à des informations conte-
nues dans un signal reçu par une station de réception abon-
né (21) comprenant des étapes :

- d'émission de premiers messages de contrôle d'allocation de droits (ECM) permettant de proposer aux abonnés un mode de fonctionnement à la demande et de seconds messages de gestion d'allocation de droits (EMM) vers un dispositif utilisateur (26),

- de génération dans le dispositif utilisateur (26) d'un signal d'autorisation d'accès (CW),

dans lequel on émet des premiers messages de contrôle d'allocation de droits (ECM) ayant un contenu de profil paramétrable permettant de faire une offre additionnelle pour au moins un service ou un programme à un abonné en fonction de son profil.



FR 2 848 764 - A1



(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international(43) Date de la publication internationale
8 juillet 2004 (08.07.2004)

PCT

(10) Numéro de publication internationale
WO 2004/057871 A2(51) Classification internationale des brevets⁷ :

H04N 7/167

Jean-Luc [FR/FR]; 19 rue Eugène Manuel, F-75116
PARIS (FR).

(21) Numéro de la demande internationale :

PCT/FR2003/050181

(81) États désignés (*national*) : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(22) Date de dépôt international :

16 décembre 2003 (16.12.2003)

(25) Langue de dépôt :

français

(26) Langue de publication :

français

(30) Données relatives à la priorité :

02 15978 17 décembre 2002 (17.12.2002) FR

(71) Déposant (*pour tous les États désignés sauf US*) : CANAL
+ TECHNOLOGIES [FR/FR]; 34 Place Raoul Dautry,
F-75015 PARIS (FR).(84) États désignés (*régional*) : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

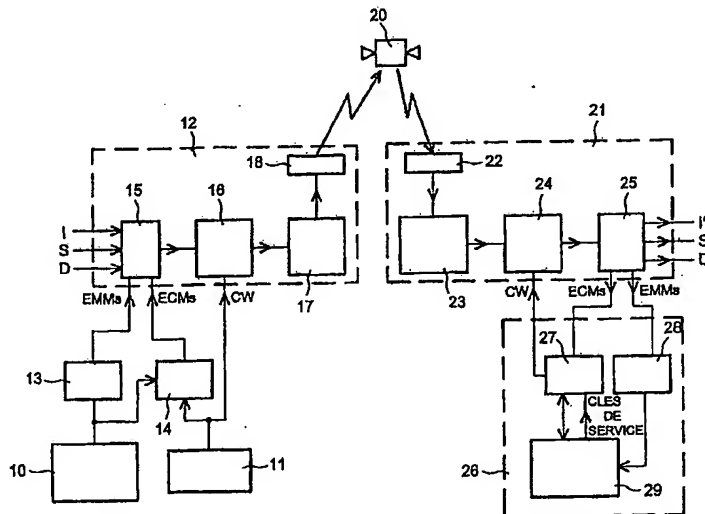
(72) Inventeur; et

(75) Inventeur/Déposant (*pour US seulement*) : DAUVOIS,

[Suite sur la page suivante]

(54) Title: METHOD FOR ACCESS CONTROL IN DIGITAL PAY TELEVISION

(54) Titre : PROCÉDE DE CONTRÔLE D'ACCÈS EN TÉLÉVISION NUMÉRIQUE PAYANTS



(57) Abstract: The invention concerns a method for controlling access, in digital pay television, to data contained in the signal received by a subscriber receiving station (21) comprising steps which consist in transmitting first right allocation control messages (ECM) enabling proposal to subscribers of an on-demand operation mode and second right allocation management messages (EMM) to a user device (26), generating in the user device an access authorization signal (CW), wherein first right allocation control messages are transmitted having a parameterable profile content enabling at least one service or one programme to be authorized during a time slot based on the profile of a specific subscriber, so as to ensure an interactivity between the content of said first messages and the content of the user's device in terms of subscription for the subscriber.

[Suite sur la page suivante]

①9 RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
PARIS

①1 N° de publication : 2 838 206
(à n'utiliser que pour les
commandes de reproduction)

②1 N° d'enregistrement national : 02 04321

⑤1 Int Cl⁷ : G 06 F 12/14, H 04 L 9/32, G 06 K 19/07

⑫

DEMANDE DE BREVET D'INVENTION

A1

②2 Date de dépôt : 08.04.02.

③0 Priorité :

④3 Date de mise à la disposition du public de la
demande : 10.10.03 Bulletin 03/41.

⑤6 Liste des documents cités dans le rapport de
recherche préliminaire : *Se reporter à la fin du
présent fascicule*

⑥0 Références à d'autres documents nationaux
apparentés :

⑦1 Demandeur(s) : CANAL + TECHNOLOGIES Société
anonyme — FR.

⑦2 Inventeur(s) : DAUVOIS JEAN LUC.

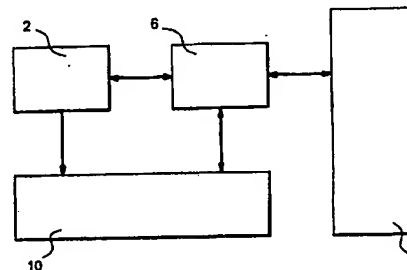
⑦3 Titulaire(s) :

⑦4 Mandataire(s) : BREVALEX.

⑤4 PROCEDE ET DISPOSITIF DE PROTECTION DE DONNEES NUMERIQUES STOCKEES DANS UNE MEMOIRE.

⑤7 L'invention concerne un procédé de protection de
données numériques stockées dans une mémoire (4) et
préalablement cryptées par une clé de chiffrement.

Le procédé selon l'invention est caractérisé par le fait
que ladite clé de chiffrement est définie dynamiquement en
fonction d'au moins un paramètre de fonctionnement intrin-
sèque à ladite carte à puce.



FR 2 838 206 - A1



(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international(43) Date de la publication internationale
16 octobre 2003 (16.10.2003)

PCT

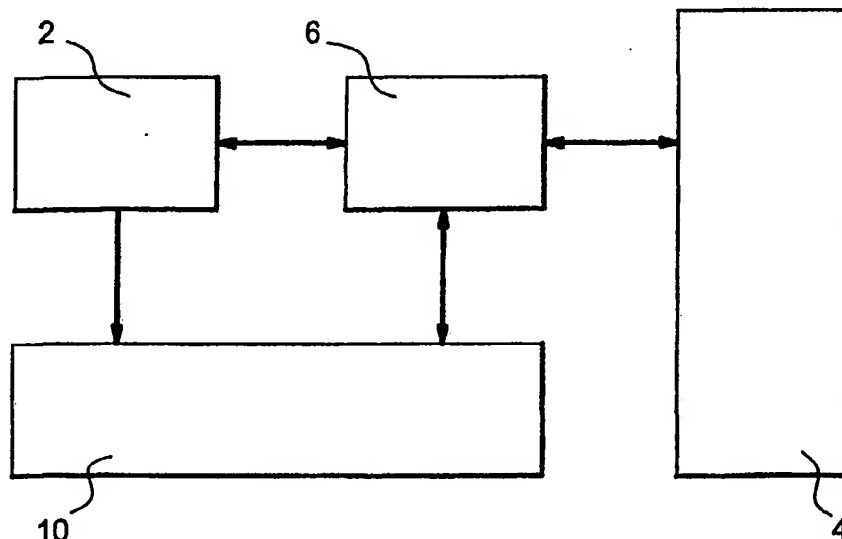
(10) Numéro de publication internationale
WO 03/085496 A1

- (51) Classification internationale des brevets⁷ : G06F 1/00 Jean Luc [FR/FR]; 19, rue Eugène Manuel, F-75116 Paris (FR).
- (21) Numéro de la demande internationale : PCT/FR03/01024 (74) Mandataire : DU BOISBAUDRY, Dominique; c/o Brevaux, 3, rue du Docteur Lancereaux, F-75008 Paris (FR).
- (22) Date de dépôt international : 2 avril 2003 (02.04.2003)
- (25) Langue de dépôt : français (81) États désignés (*national*) : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KB, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (26) Langue de publication : français (84) États désignés (*régional*) : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK,
- (30) Données relatives à la priorité : 02/04321 8 avril 2002 (08.04.2002) FR
- (71) Déposant (*pour tous les États désignés sauf US*) : CANAL + TECHNOLOGIES [FR/FR]; 34, place Raoul Dautry, F-75015 Paris (FR).
- (72) Inventeur; et
- (75) Inventeur/Déposant (*pour US seulement*) : DAUVOIS,

[Suite sur la page suivante]

(54) Title: METHOD AND DEVICE FOR PROTECTING DIGITAL DATA STORED IN A MEMORY

(54) Titre : PROCÉDE ET DISPOSITIF DE PROTECTION DE DONNÉES NUMÉRIQUES STOCKÉES DANS UNE MÉMOIRE



(57) Abstract: The invention concerns a method for protecting digital data stored in a memory (4) and previously encrypted with an encryption key. The inventive method is characterized in that said encryption key is dynamically defined on the basis of at least one operating parameter intrinsic to said smart card.

[Suite sur la page suivante]

(19) RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
PARIS

(11) N° de publication :
(à n'utiliser que pour les
commandes de reproduction)

2 850 822

(21) N° d'enregistrement national : 03 01243

(51) Int Cl⁷ : H 04 N 7/16

(12)

DEMANDE DE BREVET D'INVENTION

A1

(22) Date de dépôt : 04.02.03.

(30) Priorité :

(43) Date de mise à la disposition du public de la
demande : 06.08.04 Bulletin 04/32.

(56) Liste des documents cités dans le rapport de
recherche préliminaire : *Se reporter à la fin du
présent fascicule*

(60) Références à d'autres documents nationaux
apparentés :

(71) Demandeur(s) : CANAL + TECHNOLOGIES Société
anonyme — FR.

(72) Inventeur(s) : DAUVOIS JEAN LUC.

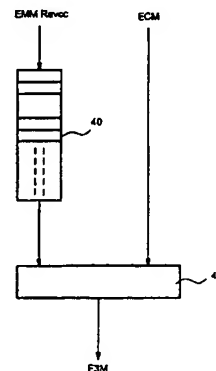
(73) Titulaire(s) :

(74) Mandataire(s) : THOMSON.

(54) SYSTEME DE TELEVISION A PEAGE, PROCEDE DE REVOCATION DE DROITS DANS UN TEL SYSTEME,
DECODEUR ET CARTE A PUCE ASSOCIES, ET MESSAGE TRANSMIS A UN TEL DECODEUR.

(57) La présente invention concerne un procédé de révo-
cation de droits d'accès à un programme audiovisuel reçu
par un décodeur (11) comprenant des étapes:

- d'émission de premiers messages (ECM) contenant
des mots de contrôle cryptés, chaque mot de contrôle (CW)
étant utilisé pour désambrouiller durant une période de
temps donné le signal audiovisuel reçu, de seconds messa-
ges (EMM) comprenant chacun des informations d'alloca-
tion de droits de l'utilisateur,
- de décryptage dans le décodeur, ou un objet portable
qui lui est associé, des premiers messages pour produire
des mots de contrôle (CW) pour le désambrouillage dudit si-
gnal audiovisuel reçu par le décodeur (11),
- d'émission de troisièmes messages hybrides résultant
chacun de la combinaison d'au moins un mot de contrôle
crypté, d'une adresse de décodeur et d'une information de
révocation de droits.



FR 2 850 822 - A1



(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international(43) Date de la publication internationale
19 août 2004 (19.08.2004)

PCT

(10) Numéro de publication internationale
WO 2004/071087 A1(51) Classification internationale des brevets⁷ : H04N 7/16,
7/167(71) Déposant (pour tous les États désignés sauf US) : CANAL
+ TECHNOLOGIES [FR/FR]; 34 place Raoul Daury,
F-75015 Paris (FR).

(21) Numéro de la demande internationale :

PCT/BP2004/050060

(72) Inventeur; et

(75) Inventeur/Déposant (pour US seulement) : DAUVOIS,
Jean-Luc [FR/FR]; 19 rue Eugène Manuel, F-75116 Paris
(FR).

(22) Date de dépôt international :

30 janvier 2004 (30.01.2004)

(25) Langue de dépôt :

français

(74) Mandataire : WEIHS, Bruno; Rosenthal & Osha, 121,
Avenue des Champs Élysées, F-75008 Paris (FR).

(26) Langue de publication :

français

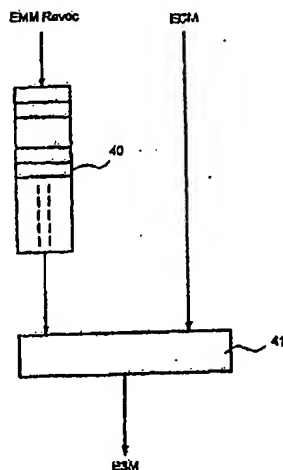
(81) États désignés (sauf indication contraire, pour tout titre de
protection nationale disponible) : AE, AG, AL, AM, AT,
AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO,

(30) Données relatives à la priorité :

0301243

4 février 2003 (04.02.2003) FR

[Suite sur la page suivante]

(54) Title: PAY TELEVISION, METHOD FOR REVOKING RIGHTS IN SUCH A SYSTEM; ASSOCIATED DECODER AND
SMART CARD, AND MESSAGE TRANSMITTED TO SUCH A DECODER(54) Titre : SYSTEME DE TELEVISION A PEAGE, PROCÉDE DE REVOCATION DE DROITS DANS UN TEL SYSTEME,
DÉCODEUR ET CARTE A PUCE ASSOCIÉS, ET MESSAGE TRANSMIS A UN TEL DÉCODEUR

ECM...ENTITLEMENT CONTROL MESSAGE

E3M...HYBRID MESSAGE

EMM REVOC...RIGHT REVOCATION MESSAGE

(57) Abstract: The invention concerns a method for revoking access rights to an audio-visual programme received by a decoder (11) comprising the following steps: transmitting first messages (ECM) containing encrypted control words, each control word (CW) being used to descramble for a given time period the audio-visual signal received, second messages (E3M) comprising each data allocating user rights; decrypting in the decoder, or a portable object associated therewith, the first messages to produce control words (CW) for descrambling said audio-visual signal received by the decoder (11), transmitting third hybrid messages resulting each from the combination of at least one encrypted control word (CW), a decoder address and a right revoking information.

(57) Abrégé : La présente invention concerne un procédé de révocation de droits d'accès à un programme audiovisuel reçu par un décodeur (11) comprenant des étapes : - d'émission de premiers messages (ECM) contenant des mots de contrôle cryptés, chaque mot de contrôle (CW) étant utilisé pour désambrouiller durant une période de temps donné le signal

audiovisuel reçu, de seconds messages (E3M) comprenant chacun des informations d'allocation de droits de l'utilisateur, - de décryptage dans le décodeur, ou un objet portable qui lui est associé, des premiers messages pour produire des mots de contrôle (CW) pour le désambrouillage dudit signal audiovisuel reçu par le décodeur (11), - d'émission de troisièmes messages hybrides résultant

[Suite sur la page suivante]

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international(43) Date de la publication internationale
23 septembre 2004 (23.09.2004)

PCT

(10) Numéro de publication internationale
WO 2004/082286 A1(51) Classification internationale des brevets⁷ :
H04N 7/167(74) Mandataire : WEIHS, Bruno; Osha Novak & May, 121
avenue des Champs Elysées, F-75008 Paris (FR).(21) Numéro de la demande internationale :
PCT/EP2004/050299(81) États désignés (sauf indication contraire, pour tout titre de
protection nationale disponible) : AE, AG, AL, AM, AT,
AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO,
CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB,
GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG,
KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG,
MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH,
PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(22) Date de dépôt international : 12 mars 2004 (12.03.2004)

(25) Langue de dépôt : français

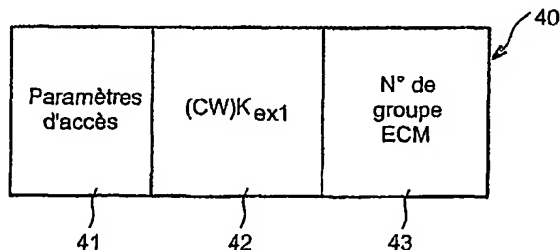
(26) Langue de publication : français

(30) Données relatives à la priorité :
03/50044 12 mars 2003 (12.03.2003) FR(71) Déposant (pour tous les États désignés sauf US) :
CANAL+ TECHNOLOGIES [FR/FR]; 34 Place Raoul
Dautry, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : DAUVOIS,
Jean-Luc [FR/FR]; 19 rue Eugène Manuel, F-75116 Paris
(FR). CASSAGNE, Philippe [FR/FR]; 18 rue du Bourg
Tibourg, F-75004 Paris (FR).(84) États désignés (sauf indication contraire, pour tout titre de
protection régionale disponible) : ARIPO (BW, GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien
(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT,
BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR,
HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR),
OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML,
MR, NE, SN, TD, TG).

[Suite sur la page suivante]

(54) Title: PAY TELEVISION SYSTEM, METHOD FOR TRANSMISSION OF SCRAMBLED AUDIOVISUAL PRO-
GRAMMMES, DECODER AND CHIP FOR CARRYING OUT SAID METHOD(54) Titre : SYSTEME DE TELEVISION A PEAGE, PROCEDE DE DIFFUSION DE PROGRAMMES AUDIOVISUELS
BROUILLES, DECODEUR ET CARTE A PUCES METTANT EN OEUVRE CE PROCEDE

41... ACCESS PARAMETERS

43... NUMBER OF THE ECM GROUP

(57) Abstract: The invention relates to a method
for broadcasting a scrambled audiovisual programme
to decoders (11), comprising a step for transmission
of first messages (ECM) to said decoders, each
comprising a control word (CW), encrypted using a
operation key permitting each decoder to unscramble
the received audiovisual programme during a given
period, second messages (EMM) comprising operation
keys according to which during the same basic period
as the scrambling time for the scrambled audiovisual
programme, there is transmission of at least two first
messages, each containing the same control word
respectively encrypted by distinct operation keys
and second messages, each containing one of said
operation keys and an individual or group address of

at least one decoder of the at least two decoder units.

(57) Abrégé : La présente invention concerne un procédé de diffusion d'un programme audiovisuel brouillé à destination de déco-
deurs (11) comprenant une étape d'émission vers ces décodeurs de premiers messages (ECM) contenant chacun un mot de contrôle
(CW) crypté par une clé d'exploitation, pour permettre à chaque décodeur de débrouiller, durant une période de temps donnée,
le programme audiovisuel reçu, de seconds messages (EMM) comprenant des clés d'exploitation, selon lequel au cours de l'étape
d'émission, pour une même période élémentaire de temps de brouillage du programme audiovisuel brouillé, il y a émission d'au moins
deux premiers messages comprenant chacun un même mot de contrôle crypté par des clés d'exploitation distinctes respectives, et de
seconds messages qui contiennent chacun l'une de ces clés d'exploitation ainsi qu'une adresse, individuelle ou de groupe, d'au moins
un décodeur de l'un d'au moins deux ensembles de décodeurs.

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
19 août 2004 (19.08.2004)

PCT

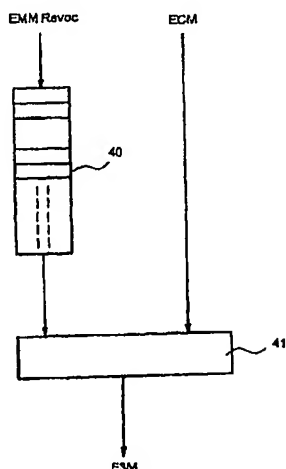
(10) Numéro de publication internationale
WO 2004/071087 A1

- (51) Classification internationale des brevets⁷ : **H04N 7/16, 7/167**
- (71) Déposant (pour tous les États désignés sauf US) : **CANAL + TECHNOLOGIES [FR/FR]**; 34 place Raoul Dautry, F-75015 Paris (FR).
- (21) Numéro de la demande internationale : **PCT/EP2004/050060**
- (72) Inventeur; et
(75) Inventeur/Déposant (pour US seulement) : **DAUVOIS, Jean-Luc [FR/FR]**; 19 rue Eugène Manuel, F-75116 Paris (FR).
- (22) Date de dépôt international : **30 janvier 2004 (30.01.2004)**
- (25) Langue de dépôt : **français**
- (74) Mandataire : **WEIHS, Bruno; Rosenthal & Osha, 121, Avenue des Champs Elysées, F-75008 Paris (FR).**
- (26) Langue de publication : **français**
- (81) États désignés (sauf indication contraire, pour tout titre de protection nationale disponible) : **AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO,**
- (30) Données relatives à la priorité : **0301243 4 février 2003 (04.02.2003) FR**

[Suite sur la page suivante]

(54) Title: **PAY TELEVISION, METHOD FOR REVOKING RIGHTS IN SUCH A SYSTEM, ASSOCIATED DECODER AND SMART CARD, AND MESSAGE TRANSMITTED TO SUCH A DECODER**

(54) Titre : **SYSTEME DE TELEVISION A PEAGE, PROCEDE DE REVOCATION DE DROITS DANS UN TEL SYSTEME, DECODEUR ET CARTE A PUCE ASSOCIES, ET MESSAGE TRANSMIS A UN TEL DECODEUR**



ECM...ENTITLEMENT CONTROL MESSAGE
E3M...HYBRID MESSAGE
EMM REVOC...RIGHT REVOCATION MESSAGE

audiovisuel reçu, de seconds messages (EMM) comprenant chacun des informations d'allocation de droits de l'utilisateur, - de décryptage dans le décodeur, ou un objet portable qui lui est associé, des premiers messages pour produire des mots de contrôle (CW) pour le désencodage dudit signal audiovisuel reçu par le décodeur (11), - d'émission de troisièmes messages hybrides résultant

(57) Abstract: The invention concerns a method for revoking access rights to an audio-visual programme received by a decoder (11) comprising the following steps: transmitting first messages (ECM) containing encrypted control words, each control word (CW) being used to descramble for a given time period the audio-visual signal received, second messages (EMM) comprising each data allocating user rights; decrypting in the decoder, or a portable object associated therewith, the first messages to produce control words (CW) for descrambling said audio-visual signal received by the decoder (11), transmitting third hybrid messages resulting each from the combination of at least one encrypted control word (CW), a decoder address and a right revoking information.

(57) Abrégé : La présente invention concerne un procédé de révocation de droits d'accès à un programme audiovisuel reçu par un décodeur (11) comprenant des étapes : - d'émission de premiers messages (ECM) contenant des mots de contrôle cryptés, chaque mot de contrôle (CW) étant utilisé pour désencodage durant une période de temps donné le signal

[Suite sur la page suivante]

WO 2004/071087 A1

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
8 juillet 2004 (08.07.2004)

PCT

(10) Numéro de publication internationale
WO 2004/057871 A2

(51) Classification internationale des brevets⁷ :
H04N 7/167

Jean-Luc [FR/FR]; 19 rue Eugène Manuel, F-75116
PARIS (FR).

(21) Numéro de la demande internationale :
PCT/FR2003/050181

(22) Date de dépôt international :
16 décembre 2003 (16.12.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02 15978 17 décembre 2002 (17.12.2002) FR

(71) Déposant (pour tous les États désignés sauf US) : CANAL
+ TECHNOLOGIES [FR/FR]; 34 Place Raoul Dautry,
F-75015 PARIS (FR).

(72) Inventeur; et

(75) Inventeur/Déposant (pour US seulement) : DAUVOIS,

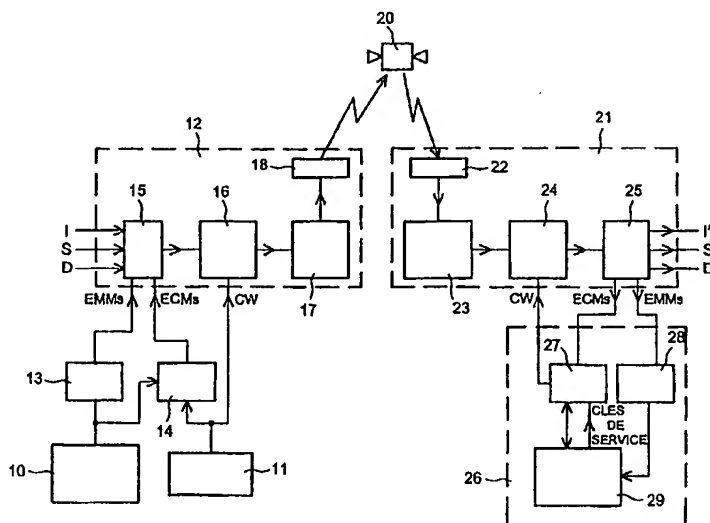
(81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,
DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH,
GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC,
LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW,
MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC,
SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés (régional) : brevet ARIPO (GH, GM, KE,
LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet
eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet
européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK,
TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,
GW, ML, MR, NE, SN, TD, TG).

[Suite sur la page suivante]

(54) Title: METHOD FOR ACCESS CONTROL IN DIGITAL PAY TELEVISION

(54) Titre : PROCEDE DE CONTROLE D'ACCES EN TELEVISION NUMERIQUE PAYANTS



(57) Abstract: The invention concerns a method for controlling access, in digital pay television, to data contained in the signal received by a subscriber receiving station (21) comprising steps which consist in transmitting first right allocation control messages (ECM) enabling proposal to subscribers of an on-demand operation mode and second right allocation management messages (EMM) to a user device (26), generating in the user device an access authorization signal (CW), wherein first right allocation control messages are transmitted having a parameterable profile content enabling at least one service or one programme to be authorized during a time slot based on the profile of a specific subscriber, so as to ensure an interactivity between the content of said first messages and the content of the user's device in terms of subscription for the subscriber.

[Suite sur la page suivante]

WO 2004/057871 A2

(12) DEMANDE INTERNATIONALE PUBLÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
13 mai 2004 (13.05.2004)

PCT

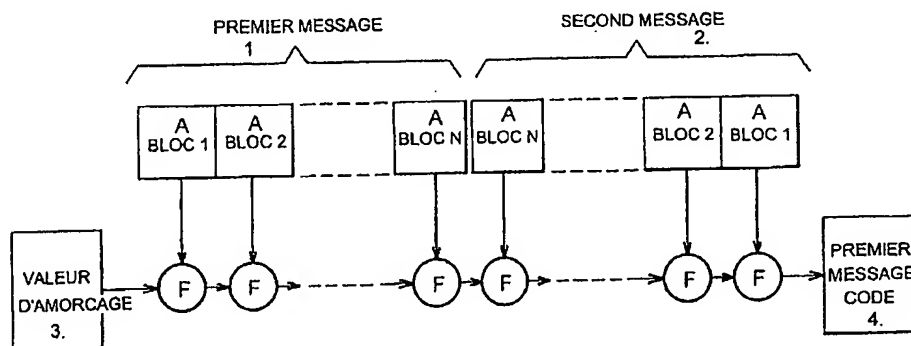
(10) Numéro de publication internationale
WO 2004/040818 A2

- (51) Classification internationale des brevets⁷ : H04L (72) Inventeurs; et
(21) Numéro de la demande internationale : PCT/FR2003/050104 (75) Inventeurs/Déposants (pour US seulement) : DAUVOIS,
Jean-Luc [FR/FR]; 19, rue Eugène Manuel, F-75116
PARIS (FR). SAGGIORI, Jan [FR/FR]; c/o CANAL +
TECHNOLOGIES, 34, place Raoul Dautry, F-75906 Paris
Cedex 15 (FR). KOZLOV, Andrey [FR/FR]; c/o CANAL
+ TECHNOLOGIES, 34, place Raoul Dautry, F-75906
Paris Cedex 15 (FR).
(22) Date de dépôt international : 23 octobre 2003 (23.10.2003)
(25) Langue de dépôt : français
(26) Langue de publication : français (74) Mandataire : KOHRS, Martin; THOMSON, 46, Quai
Alphonse Le Gallo, F-92100 Boulogne-Billancourt (FR).
(30) Données relatives à la priorité : 02/13368 25 octobre 2002 (25.10.2002) FR (81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,
DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH,
GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC,
LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW,

[Suite sur la page suivante]

(54) Title: METHOD FOR THE SECURE TRANSMISSION OF MESSAGES OR DATA BETWEEN TWO ENTITIES

(54) Titre : PROCÉDE DE TRANSMISSION SECURISEE DE MESSAGES OU DE DONNEES ENTRE DEUX ENTITES



- 1...FIRST MESSAGE
2...SECOND MESSAGE
3...INITIATION VALUE
4...FIRST CODED MESSAGE
A...BLOCK

(57) Abstract: The invention relates to a method for the secure transmission of messages or data between two entities, involving the block coding of messages. According to the invention, a first message is broken down into a whole number N of blocks, each block being applied to an elementary coding unit of a plurality N of cascaded coding units. A second message is generated comprising the N blocks from the first message which are disposed in a different order and the 2N blocks from the first and second messages are applied to 2N cascaded coding units in order to generate the coded value which is associated with the first message.

(57) Abrégé : L'invention concerne un procédé de transmission sécurisée de messages, ou de données, entre deux entités qui est un procédé de codage par blocs de messages, dans lequel un premier message est décomposé en un nombre entier N de blocs, chaque bloc étant appliqué à une unité élémentaire de codage

[Suite sur la page suivante]

WO 2004/040818 A2

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
12 septembre 2003 (12.09.2003)

PCT

(10) Numéro de publication internationale
WO 03/075233 A2

(51) Classification internationale des brevets⁷ : G07F 7/10

Jean-Luc [FR/FR]; 19 rue Eugène Manuel, F-75116
PARIS (FR).

(21) Numéro de la demande internationale :

PCT/FR03/00637

(74) Mandataire : DU BOISBAUDRY, Dominique; c/o
BREVALEX, 3 rue du Docteur Lancereaux, F-75008
PARIS (FR).

(22) Date de dépôt international :

27 février 2003 (27.02.2003)

(25) Langue de dépôt :

français

(26) Langue de publication :

français

(30) Données relatives à la priorité :

02/02620

1 mars 2002 (01.03.2002) FR

(71) Déposant (pour tous les États désignés sauf US) : CANAL
+ TECHNOLOGIES [FR/FR]; 34 Place Raoul Dautry,
F-75015 PARIS (FR).

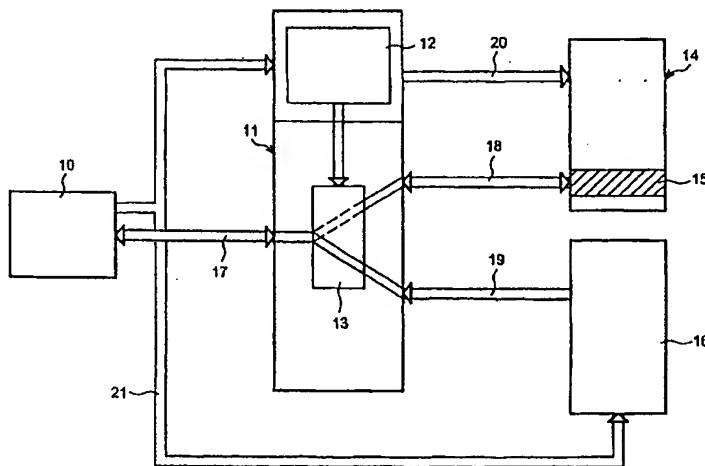
(81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,
DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM,
HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK,
LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX,
MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG,
SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC,
VN, YU, ZA, ZM, ZW.

(84) États désignés (régional) : brevet ARIPO (GH, GM, KE,
LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet
eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet
européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,

[Suite sur la page suivante]

(54) Title: SMART CARD AND METHOD FOR AVOIDING SOFTWARE BUG ON SUCH A SMART CARD

(54) Titre : CARTE A PUCE ET PROCÉDÉ D'ÉVITEMENT DE FAILLE LOGIQUE SUR UNE TELLE CARTE A PUCE



(57) Abstract: The invention concerns a smart card whereof the component includes a central unit (10), a code memory (16) wherein is stored an original code comprising at least a software bug which cannot be corrected, a data/code memory (14) in a zone (15) of which are stored a substitution code free of software bug, as well as the addresses of the software bug(s), a mechanism (11) for intercepting the central unit addresses which verifies the hardware addresses which are executed, wherein the mechanism (11) intercepting the addresses includes an address intercepting and substituting unit (12) which enables the central unit to be rerouted when it detects an address or a set of addresses of software bug and a data multiplexer (13) enabling either the memory code data (16) when there is no rerouting, or the data of the data/memory code (14) to be taken into account by the central unit (10). The invention also concerns a method for avoiding a software bug in such a smart card.

[Suite sur la page suivante]

WO 03/075233 A2



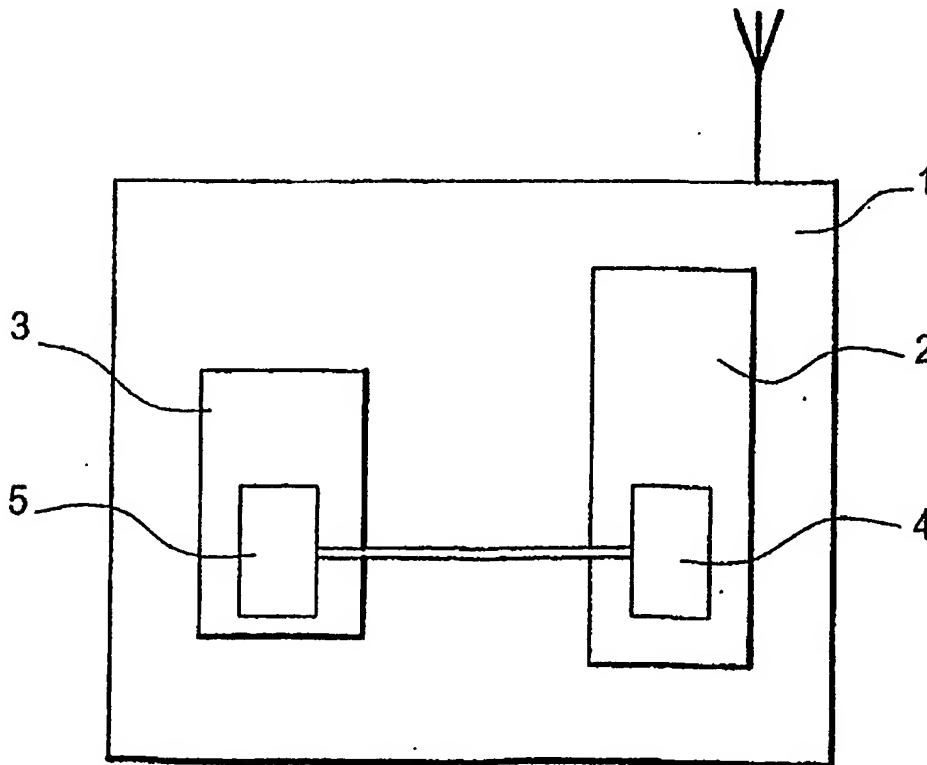
US 20050044562A1

(19) **United States**(12) **Patent Application Publication** (10) Pub. No.: **US 2005/0044562 A1**
Dauvois (43) Pub. Date: **Feb. 24, 2005**(54) **METHOD FOR VERIFYING TELEVISION
RECEIVER SETS WITH ACCESS CONTROL
AND CORRESPONDING RECEIVER SET****Publication Classification**(51) Int. Cl.⁷ **H04N 7/16; H04N 7/167**
(52) U.S. Cl. **725/25; 725/31; 725/6**(76) Inventor: **Jean-Luc Dauvois, Le Mans (FR)**(57) **ABSTRACT**Correspondence Address:
OSHA & MAY L.L.P.
1221 MCKINNEY STREET
HOUSTON, TX 77010 (US)

The invention concerns a method for verifying television receiver sets with access control and a corresponding receiver set. The invention is characterized in that a broadcaster performs parametered calculations, for example through the subscriptions and the characteristics of the receiver sets. The results of said calculations are transmitted to the receiver set which store them. In order to verify a receiver, the broadcaster transmits thereto the parameter(s) used, the receiver performs the calculation and compares the result it obtains with that which it has stored. In case of non-conformity, the receiver set modifies its operating conditions. The invention is applicable to television with access control.

(21) Appl. No.: **10/493,378**(22) PCT Filed: **Oct. 25, 2002**(86) PCT No.: **PCT/FR02/03673**(30) **Foreign Application Priority Data**

Oct. 26, 2001 (FR)..... 01/13878



(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
19 juin 2003 (19.06.2003)

PCT

(10) Numéro de publication internationale
WO 03/050756 A2

(51) Classification internationale des brevets⁷ :
G06K 19/00

(71) Déposant (pour tous les États désignés sauf US) : CANAL
+ TECHNOLOGIES [FR/FR]; 34, place Raoul Dautry,
F-75015 Paris (FR).

(21) Numéro de la demande internationale :
PCT/FR02/04284

(72) Inventeur; et
(75) Inventeur/Déposant (pour US seulement) : DAUVOIS,
Jean-Luc [FR/FR]; 19, rue Eugène Manuel, F-75116 Paris
(FR).

(22) Date de dépôt international :
11 décembre 2002 (11.12.2002)

(25) Langue de dépôt : français

(74) Mandataire : DU BOISBAUDRY, Dominique;
c/o Brevalet, 3, rue du Docteur Lancereaux, F-75008
Paris (FR).

(26) Langue de publication : français

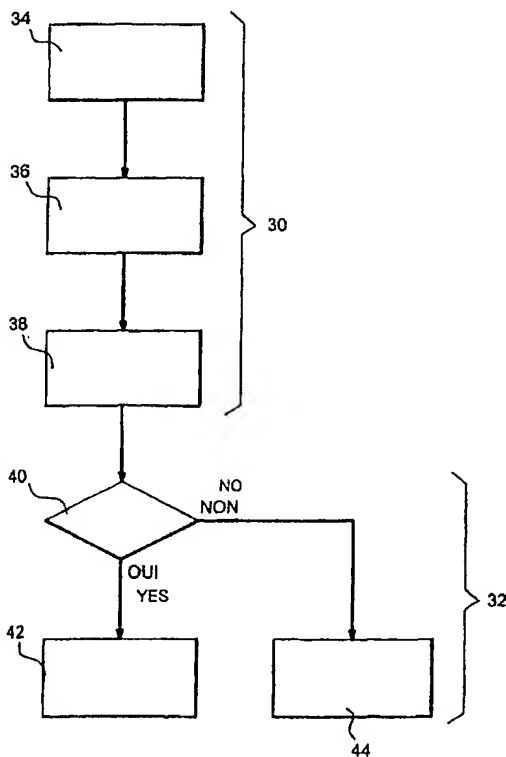
(30) Données relatives à la priorité :
01/16113 13 décembre 2001 (13.12.2001) FR

(81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,

[Suite sur la page suivante]

(54) Title: METHOD OF COMBATING THE FRAUDULENT REPRODUCTION OF CHIP CARDS AND THE READ TERMINALS FOR SAID CARDS

(54) Titre : LUTTE CONTRE LA REPRODUCTION FRAUDULEUSE DES CARTES A PUCE ET DES TERMINAUX DE LECTURE DE CES CARTES



(57) Abstract: The invention relates to a method of pairing a predefined type of card read terminal (2), comprising a central processing unit (6), with a predefined type of chip card (4) which is intended to store confidential data. The inventive method consists in: comparing (40) the electrical operating parameters of said card with specific, previously-stored electrical parameters; and authorising (42) access to the confidential data using said new memory card if the data compared are not identical.

(57) Abrégé : L'invention concerne un procédé d'appariement d'un terminal (2) de lecture de cartes d'un type prédéfini comportant une unité centrale (6) de traitement et d'une carte à puce (4) d'un type prédéfini destinée à stocker des données secrètes. Ce procédé consiste à comparer (40) des paramètres électriques de fonctionnement de cette carte avec les paramètres électriques particuliers préalablement mémorisés, et autoriser (42) l'accès aux données secrètes au moyen de cette nouvelle carte à mémoire si les données comparées sont identiques

WO 03/050756 A2

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
19 juin 2003 (19.06.2003)

PCT

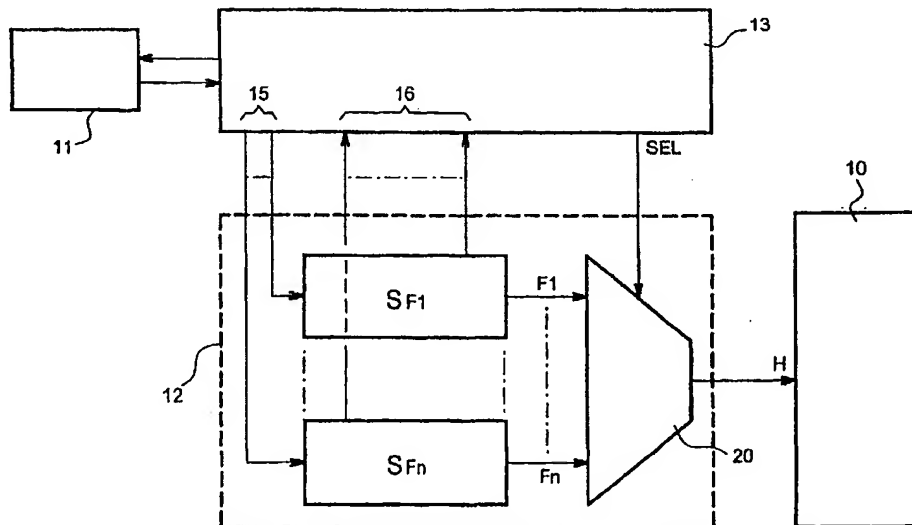
(10) Numéro de publication internationale
WO 03/050750 A1

- (51) Classification internationale des brevets⁷ : G06K 7/00, 19/07 (72) Inventeurs; et
(75) Inventeurs/Déposants (pour US seulement) : DAUVOIS, Jean-Luc [FR/FR]; 19, rue Eugène Manuel, F-75116 Paris (FR). PERRINE, Jérôme [FR/FR]; 46, rue Ancienne Mairie, F-92100 Boulogne (FR).
- (21) Numéro de la demande internationale : PCT/FR02/04285
- (22) Date de dépôt international : 11 décembre 2002 (11.12.2002) (74) Mandataire : DU BOISBAUDRY, Dominique; c/o BrevaLex, 3, rue du Docteur Lancereaux, F-75008 Paris (FR).
- (25) Langue de dépôt : français
- (26) Langue de publication : français (81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (30) Données relatives à la priorité : 01/16114 13 décembre 2001 (13.12.2001) FR
- (71) Déposant (pour tous les États désignés sauf US) : CANAL + TECHNOLOGIES [FR/FR]; 34, place Raoul Dautry, F-75015 Paris (FR).

[Suite sur la page suivante]

(54) Title: DIGITAL ELECTRONIC COMPONENT WHICH IS PROTECTED AGAINST ELECTRICAL-TYPE ANALYSES

(54) Titre : COMPOSANT ELECTRONIQUE NUMERIQUE PROTEGE CONTRE DES ANALYSES DE TYPE ELECTRIQUE



(57) Abstract: The invention relates to a digital electronic component which is protected against electrical- and/or electromagnetic-type analyses. The inventive component comprises: a synchronous element (10) which is controlled by a clock (H); means (11, 12) of generating said clock (H), the frequency of which varies randomly between a minimum value and a maximum value for at least a given period of time; and means (13) of controlling the random nature of the frequency change of said clock (H).

[Suite sur la page suivante]

WO 03/050750 A1

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
1 mai 2003 (01.05.2003)

PCT

(10) Numéro de publication internationale
WO 03/036974 A2

(51) Classification internationale des brevets⁷ : H04N 7/16

(21) Numéro de la demande internationale :
PCT/FR02/03673

(22) Date de dépôt international :
25 octobre 2002 (25.10.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
01/13878 26 octobre 2001 (26.10.2001) FR

(71) Déposant (pour tous les États désignés sauf US) : CANAL
+ TECHNOLOGIES [FR/FR]; 34, Place Raoul Dautry,
F-75015 Paris (FR).

(72) Inventeur; et

(75) Inventeur/Déposant (pour US seulement) : DAUVOIS,
Jean-Luc [FR/FR]; 19, rue Eugène Manuel, F-75116 Paris
(FR).

(74) Mandataire : DU BOISBAUDRY, Dominique; Brevaux,
3, rue du Docteur Lancereaux, F-75008 Paris (FR).

(81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,
DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM,
HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK,
LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX,
MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI,
SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC,
VN, YU, ZA, ZM, ZW.

(84) États désignés (régional) : brevet ARIPO (GH, GM, KE,
LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet
eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet
européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), brevet
OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML,
MR, NE, SN, TD, TG).

Publiée :

— sans rapport de recherche internationale, sera republiée
dès réception de ce rapport

En ce qui concerne les codes à deux lettres et autres abrévia-
tions, se référer aux "Notes explicatives relatives aux codes et
abréviations" figurant au début de chaque numéro ordinaire de
la Gazette du PCT.

(54) Title: METHOD FOR VERIFYING TELEVISION RECEIVER SETS WITH ACCESS CONTROL AND CORRESPOND-
ING RECEIVER SET

(54) Titre : PROCEDE DE VERIFICATION DE RECEPTEURS DE TELEVISION A CONTROLE D'ACCES ET RECEPTEUR
CORRESPONDANT

(57) Abstract: The invention concerns a method for verifying television receiver sets with access control and a corresponding receiver set. The invention is characterized in that a broadcaster performs parametered calculations, for example through the sub-
scriptions and the characteristics of the receiver sets. The results of said calculations are transmitted to the receiver set which store
them. In order to verify a receiver, the broadcaster transmits thereto the parameter(s) used, the receiver performs the calculation
and compares the result it obtains with that which it has stored. In case of non-conformity, the receiver set modifies its operating
conditions. The invention is applicable to television with access control.

(57) Abrégé : Procédé de vérification de récepteurs de télévision à contrôle d'accès et récepteur correspondant. Selon l'invention,
un diffuseur effectue des calculs paramétrés, par exemple par les abonnements et les caractéristiques des récepteurs. Les résultats de
ces calculs sont transmis aux récepteurs, qui les stockent. Pour vérifier un récepteur, le diffuseur lui transmet le ou les paramètres
utilisés, le récepteur effectue le calcul et compare le résultat qu'il obtient avec celui qu'il stocke. En cas de désaccord, le récepteur
modifie son fonctionnement. Application en télévision à contrôle d'accès.

WO 03/036974 A2

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
10 octobre 2002 (10.10.2002)

PCT

(10) Numéro de publication internationale
WO 02/080544 A1

(51) Classification internationale des brevets⁷ : H04N 7/16,
7/167

(71) Déposant (pour tous les États désignés sauf US) : CANAL
+ TECHNOLOGIES [FR/FR]; 34, place Raoul Dautry,
F-75015 Paris (FR).

(21) Numéro de la demande internationale :
PCT/FR02/01010

(72) Inventeurs; et
(75) Inventeurs/Déposants (pour US seulement) : DAUVOIS,
Jean-Luc [FR/FR]; 19, rue Eugène Manuel, F-75116 Paris
(FR). MAILLARD, Michel [FR/FR]; 13, avenue du Parc,
F-78120 Rambouillet (FR).

(22) Date de dépôt international : 22 mars 2002 (22.03.2002)

(25) Langue de dépôt : français

(74) Mandataire : POULIN, Gérard; c/o Brevaux, 3, rue du
Docteur Lancereaux, F-75008 Paris (FR).

(26) Langue de publication : français

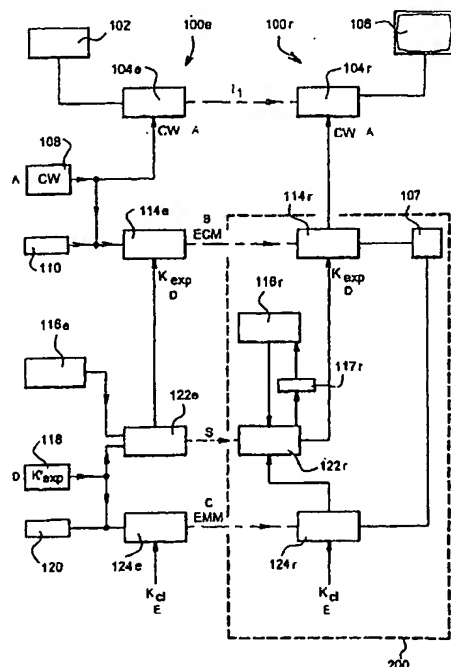
(30) Données relatives à la priorité :
01/04342 30 mars 2001 (30.03.2001) FR

(81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,

[Suite sur la page suivante]

(54) Title: SYSTEM AND METHOD FOR TRANSMITTING ENCRYPTED DATA WITH ENCRYPTION KEY

(54) Titre : SYSTEME ET PROCEDE DE TRANSMISSION D'INFORMATIONS CHIFFREES A CLE CHIFFREE



104e, 114e, 116e, 122e, 124e... ENCRYPTION UNITS
104r, 114r, 116r, 122r, 124r... DECRYPTION UNITS
A... ENCODING KEY
B... ENTITLEMENT CONTROL MESSAGE

C... ENTITLEMENT MANAGEMENT MESSAGE
D... OPERATING KEY
E... CLIENT KEY
S... COMMAND MESSAGE

(57) Abstract: The invention concerns a method for data transmission between a transmitting station (100e) and a plurality of receiving stations (100r) which consists in transmitting from the transmitting station to the receiving stations data encrypted with a first key, and at least a control message transporting a second key. The invention is characterised in that the first key, used for decrypting, is recovered in each receiving station from the second key and from at least a data selected among the set of data available in the receiving stations, based on a selection command periodically transmitted between the transmitting station and the receiving station. The invention is applicable to pay television. FIG. 2: 104e, 114e, 116e, 122e, 124e ENCRYPTION UNITS 104r, 114r, 116r, 122r, 124r DECRYPTION UNITS A ENCODING KEY B ENTITLEMENT CONTROL MESSAGE C ENTITLEMENT MANAGEMENT MESSAGE D OPERATING KEY E CLIENT KEY S COMMAND MESSAGE

(57) Abrégé : La présente invention concerne un procédé de transmission d'informations entre une station émettrice (100e) et une pluralité de stations réceptrices (100r) dans lequel on transmet de la station émettrice vers la station réceptrice des informations chiffrées avec une première clé, et au moins un message de contrôle vecteur d'une deuxième clé. Conformément à l'invention,

[Suite sur la page suivante]

WO 02/080544 A1



(19) **United States**

(12) **Patent Application Publication** (10) Pub. No.: US 2004/0114764 A1
Dauvois et al. (43) Pub. Date: **Jun. 17, 2004**

Dauvois et al.

(43) Pub. Date: Jun. 17, 2004

(54) **SYSTEM AND METHODS FOR TRANSMITTING ENCRYPTED DATA WITH ENCRYPTION KEY**

Publication Classification

(51) Int. Cl.⁷ H04L 9/00

(52) U.S. Cl. 380/277

(76) Inventors: **Jean-Luc Dauvois**, Paris (FR); **Michel Maillard**, Rambouillet (FR)

Correspondence Address:
OBLON, SPIVAK, MCCLELLAND, MAIER &
NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314 (US)

(21) Appl. No.: 10/472,201

(22) PCT Filed: Mar. 22, 2002

(86) PCT No.: PCT/FR02/01010

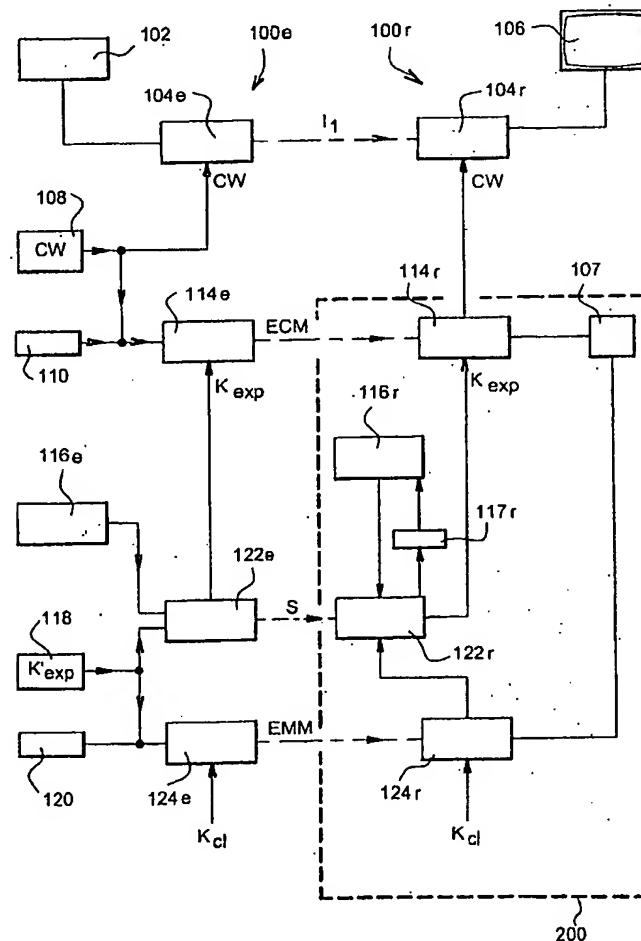
(30) Foreign Application Priority Data

Mar. 30, 2001 (FR)..... 01/04342

(57) **ABSTRACT**

The present invention relates to a method for transmitting information between a transmitter station (100e) and a plurality of receiving stations (100r) wherein encrypted information is transmitted from the transmitter station to the receiver station with a first key and at least a control message bearing a second key. According to the invention, the first key used for decryption is restored in each receiving station from the second key and from at least one datum selected from a set of data available in the receiving stations, according to a selection command periodically transmitted between the transmitting station and the receiving station.

Application to pay television.



(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
22 novembre 2001 (22.11.2001)

PCT

(10) Numéro de publication internationale
WO 01/89215 A2

(51) Classification internationale des brevets⁷ :
H04N 7/167, H04L 9/22

(71) Déposant (pour tous les États désignés sauf US) : CANAL
+ TECHNOLOGIES (FR/FR); 34, place Raoul Dautry,
F-75015 Paris (FR).

(21) Numéro de la demande internationale :
PCT/FR01/01465

(72) Inventeur; et
(75) Inventeur/Déposant (pour US seulement) : DAUVOIS,
Jean-Luc (FR/FR); 19, rue Eugène Manuel, F-75116 Paris
(FR).

(22) Date de dépôt international : 15 mai 2001 (15.05.2001)

(25) Langue de dépôt : français

(74) Mandataire : ILGART, Jean-Christophe; Brevaux, 3,
rue du Docteur Lancereaux, F-75008 Paris (FR).

(26) Langue de publication : français

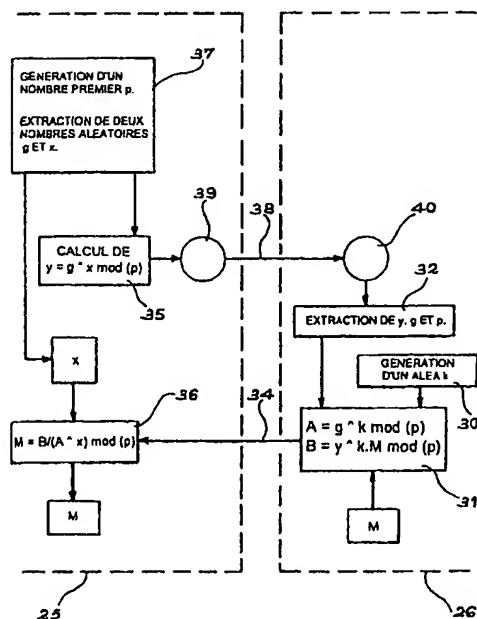
(30) Données relatives à la priorité :
00/06205 16 mai 2000 (16.05.2000) FR

(81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE,
DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU,

[Suite sur la page suivante]

(54) Title: METHOD FOR TRANSMITTING ENCRYPTED DATA, USE OF SAME IN A PAY DIGITAL TELEVISION SYSTEM AND DECODER USED IN SAID SYSTEM

(54) Titre : PROCEDE DE TRANSMISSION DE DONNEES CHIFFREES, APPLICATION D'UN TEL PROCEDE DANS UN SYSTEME DE TELEVISION NUMERIQUE A PEAGE ET DECODEUR UTILISE DANS UN TEL SYSTEME



37...GENERATING A FIRST NUMBER p.

35...CALCULATING OF $y = g^x \text{ mod } (p)$

32...RETRIEVING y, g AND p.

30...GENERATING A RANDOM VARIABLE k

(57) Abstract: The invention concerns a transmission method between a first module (25) and a second module (26) comprising the following steps: in the first module (25): calculating y such that $y = g^x \text{ mod } (p)$, g and x being the random numbers preserved in the terminal, p being a prime number, g and p being known to the two modules; transmitting (38) the value y to the second module; in the second module (26): retrieving (32) the value y; generating (30) a random variable k; calculating (31) two values A and B, such that $A = g^k \text{ mod } (p)$ $B = y^k.M \text{ mod } (p)$, M being a known message to be transmitted in encrypted form; transmitting (34) values A and B to the first module (25); in the first module (25): retrieving (36) the message M using the following formula: $M = B/(A^x) \text{ mod } (p)$.

(57) Abrégé : La présente invention concerne un procédé de transmission entre un premier module (25) et un second module (26) comprenant les étapes suivantes: dans le premier module (25): calcul de y tel que: $y = g^x \text{ mod } (p)$, g et x étant des nombres aléatoires conservés dans le terminal, p étant un nombre premier, g et p étant connus des deux modules; transmission (38) de la valeur y vers le second module, dans le second module (26): récupération (32) de la valeur y; génération (30) d'un aléa k; calcul (31) de deux valeurs A et B, telles que: $A = g^k \text{ mod } (p)$, $B = y^k.M \text{ mod } (p)$, M étant un message connu à transmettre chiffré; transmission (34) des valeurs A et B vers le premier module, dans le premier module (25): récupération (36) du message M en utilisant la formule suivante: $M = B/(A^x) \text{ mod } (p)$.



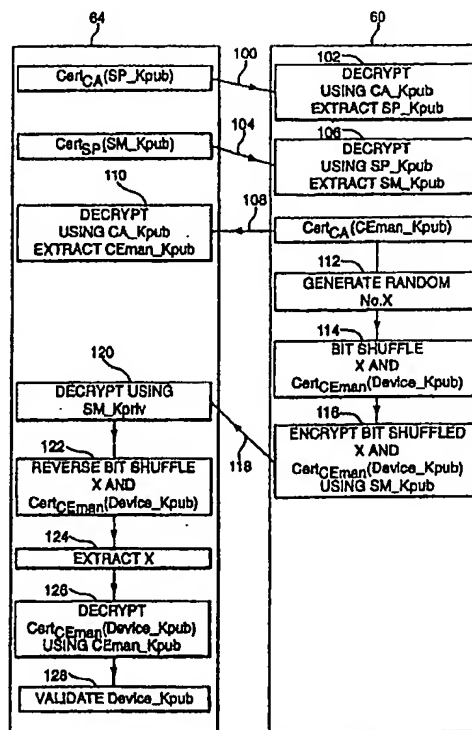
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁷ : H04N 5/913		A1	(11) International Publication Number: WO 00/62540
			(43) International Publication Date: 19 October 2000 (19.10.00)
(21) International Application Number: PCT/IB00/00432		(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).	
(22) International Filing Date: 31 March 2000 (31.03.00)			
(30) Priority Data: 99400901.7 13 April 1999 (13.04.99) EP			
(71) Applicant (for all designated States except US): CANAL+ SOCIETE ANONYME [FR/FR]; 85/89, quai André Citroën, F-75711 Paris Cedex 15 (FR).			
(72) Inventors; and (75) Inventors/Applicants (for US only): MAILLARD, Michel [FR/FR]; 42, avenue du Maréchal Leclerc, F-28130 Maintenon (FR). DAUVOIS, Jean-Luc [FR/FR]; 19, rue Eugène Manuel, F-75116 Paris (FR). DUBLANCHET, Frédéric [FR/FR]; Canal+ Technologies Société Anonyme, 34, place Raoul Dautry, F-75516 Paris Cedex 15 (FR). LEPORINI, David [FR/FR]; Canal+ Technologies Société Anonyme, 34, place Raoul Dautry, F-75516 Paris Cedex 15 (FR).		Published With international search report.	
(74) Agents: COZENS, Paul, Dennis et al.; Mathys & Squire, 100 Gray's Inn Road, London WC1X 8AL (GB).			

(54) Title: METHOD OF AND APPARATUS FOR PROVIDING SECURE COMMUNICATION OF DIGITAL DATA BETWEEN DEVICES

(57) Abstract

The present invention provides a method of providing secure communication of digital data between devices, said method comprising the steps of communicating from one device an identifier of a device to an independent security module and performing device validation depending on the identity of the received identifier.





US006904522B1

(12) **United States Patent**
Benardeau et al.

(10) Patent No.: **US 6,904,522 B1**
(45) Date of Patent: **Jun. 7, 2005**

(54) **METHOD AND APPARATUS FOR SECURE COMMUNICATION OF INFORMATION BETWEEN A PLURALITY OF DIGITAL AUDIOVISUAL DEVICES**

FOREIGN PATENT DOCUMENTS

FR	2 732 537	10/1996
WO	WO 97/35430	9/1997
WO	WO 97/38530	10/1997

OTHER PUBLICATIONS

Paper: 2244 Research Disclosure No. 335, Emsworth, GB, entitled "Encryption of Information to be recorded so as to prevent unauthorized playback", anonymous, dated Mar., 1992, 1 page.

W. Ford & B. O'Higgins; "Public-Key Cryptography and Open Systems Interconnection" IEEE Communications Magazine, vol. 30, No. 7, Jul., 1992, 6 pages.

Gerald J. Popek and Charles S. Kline, "Encryption and Secure Computer Networks", Computing Surveys, vol. 11, No. 4, Dec., 1979, 26 pages.

Patent Abstracts of Japan, English translation of abstract, "System for Transmitting Key of Encryptor", Publication No. 59067747, Date of Publication Apr. 17, 1984, one page.

* cited by examiner

Primary Examiner—Thomas R. Peeso

(74) Attorney, Agent, or Firm—Osha & May L.L.P.

(75) Inventors: Christian Benardeau, Bussy Saint Georges (FR); Jean-Luc Dauvois, Paris (FR)

(73) Assignee: Canal+ Technologies, Paris (FR)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: 09/744,040

(22) PCT Filed: Jul. 14, 1999

(86) PCT No.: PCT/IB99/01323

§ 371 (c)(1),
(2), (4) Date: Mar. 26, 2001

(87) PCT Pub. No.: WO00/04718

PCT Pub. Date: Jan. 27, 2000

(30) Foreign Application Priority Data

Jul. 15, 1998	(EP)	98401778
Jul. 22, 1998	(EP)	98401870

(51) Int. Cl.⁷ G06F 1/24

(52) U.S. Cl. 713/156; 713/168; 713/171;
713/175; 713/200; 713/201; 380/232; 380/239

(58) Field of Search 713/156, 168,
713/171, 175, 200, 201; 380/232, 239

(56) References Cited

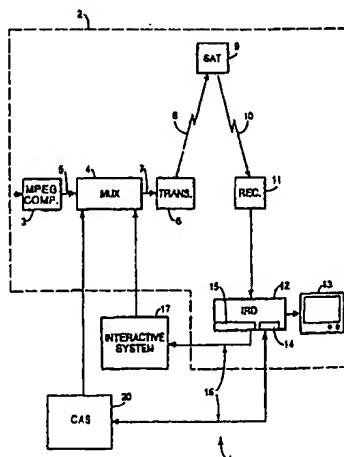
U.S. PATENT DOCUMENTS

4,633,309 A	* 12/1986	Li et al.	380/242
5,461,675 A	* 10/1995	Diehl et al.	380/229
5,509,073 A	* 4/1996	Monnin	380/229
5,563,948 A	* 10/1996	Diehl et al.	380/229
5,748,732 A	5/1998	Le Berre et al.	380/10

ABSTRACT

The present invention relates to a method of providing secure communication of information between at least a first and second digital audiovisual device (30, 52) and characterized in that the first device (30) communicates to the second device (52) a certificate $C_k(K_{pubT})$ comprising a transport public key K_{pubT} encrypted by a management private key K_{priMan} , the second device (52) decrypting the certificate using an equivalent management public key K_{pubMan} and thereafter using the transport public key K_{pubT} to encrypt information sent to the first device, the first device using an equivalent private key K_{priT} to decrypt the information. The present invention is particularly applicable to a method of providing secure communication between a first and second decoder.

51 Claims, 8 Drawing Sheets





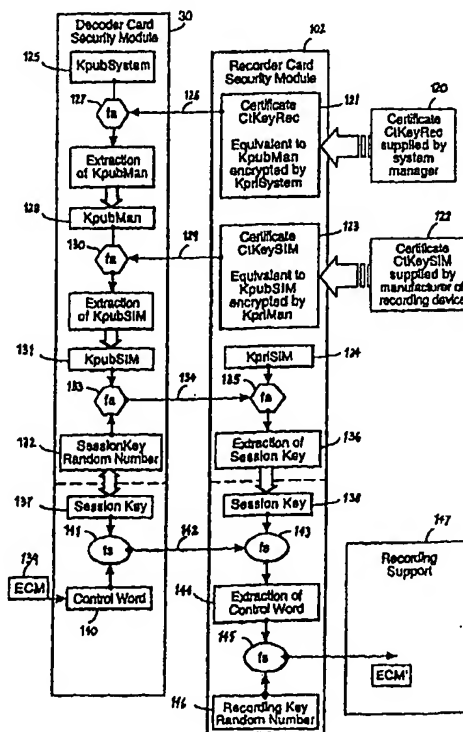
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04N 7/167, H04L 29/06		A1	(11) International Publication Number: WO 00/04718
			(43) International Publication Date: 27 January 2000 (27.01.00)
(21) International Application Number: PCT/IB99/01323			(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).
(22) International Filing Date: 14 July 1999 (14.07.99)			
(30) Priority Data:			
98401778.0	15 July 1998 (15.07.98)	EP	
98401870.5	22 July 1998 (22.07.98)	EP	
(71) Applicant (for all designated States except US): CANAL+ SOCIETE ANONYME [FR/FR]; 85/89, quai André Citroën, F-75711 Paris Cedex 15 (FR).			
(72) Inventors; and			Published With international search report.
(75) Inventors/Applicants (for US only): DAUVOIS, Jean-Luc [FR/FR]; 19, rue Eugène Manuel, F-75116 Paris (FR). BENARDEAU, Christian [FR/FR]; 13, allée des Puisatiers, F-77600 Bussy Saint Georges (FR).			
(74) Agents: COZENS, Paul, Dennis et al.; Mathys & Squire, 100 Gray's Inn Road, London WC1X 8AL (GB).			

(54) Title: METHOD AND APPARATUS FOR SECURE COMMUNICATION OF INFORMATION BETWEEN A PLURALITY OF DIGITAL AUDIOVISUAL DEVICES

(57) Abstract

The present invention relates to a method of providing secure communication of information between at least a first and second digital audiovisual device (30, 52) and characterised in that the first device (30) communicates to the second device (52) a certificate Ct(KpubT) comprising a transport public key KpubT encrypted by a management private key KpriMan, the second device (52) decrypting the certificate using an equivalent management public key KpubMan and thereafter using the transport public key KpubT to encrypt information sent to the first device, the first device using an equivalent private key KpriT to decrypt the information. The present invention is particularly applicable to a method of providing secure communication between a first and second decoder.



PCT

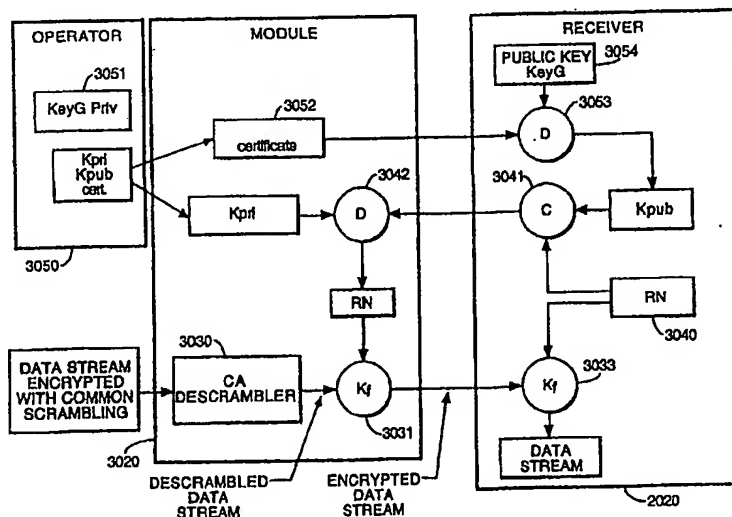
WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04N 7/16, 7/167		A1	(11) International Publication Number: WO 99/18729 (43) International Publication Date: 15 April 1999 (15.04.99)
(21) International Application Number: PCT/IB98/01610 (22) International Filing Date: 2 October 1998 (02.10.98) (30) Priority Data: 97402322.8 2 October 1997 (02.10.97) EP 98401388.8 9 June 1998 (09.06.98) EP 98401389.6 9 June 1998 (09.06.98) EP (71) Applicant (for all designated States except US): CANAL+ SOCIETE ANONYME [FR/FR]; 85/89, quai André-Citroën, F-75711 Paris Cedex 15 (FR). (72) Inventors; and (75) Inventors/Applicants (for US only): MAILLARD, Michel [FR/FR]; 42, avenue du Maréchal-Leclerc, F-28130 Maintenon (FR). BENARDEAU, Christian [FR/FR]; 13, allée des Puisatiers, F-77600 Bussy-Saint-Georges (FR). DAUVOIS, Jean-Luc [FR/FR]; 19, rue Eugène-Manuel, F-75116 Paris (FR). (74) Agents: COZENS, Paul, Dennis et al.; Mathys & Squire, 100 Grays Inn Road, London WC1X 8AL (GB).		(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published With international search report.	

(54) Title: METHOD AND APPARATUS FOR ENCRYPTED DATA STREAM TRANSMISSION



(57) Abstract

A method of transmission and reception of scrambled data in which the scrambled data is transmitted to a decoder (2020), the scrambled data being passed to and descrambled by a security module or smart card (3020) inserted in the decoder (2020) and characterised in that the scrambled data stream is passed from the smart card (2020) back to the decoder (3020) in an encrypted form. The encryption of the data stream may be carried out on the card (2020) or as a secondary encryption step at transmission. The data stream may correspond directly to audiovisual data descrambled in the security module or to a stream of control word data subsequently used by the decoder to descramble a transmission.

Declaration and Power of Attorney for Patent Application

Déclaration et Pouvoirs pour Demande de Brevet

French Language Declaration

22511
PATENT TRADEMARK OFFICE

En tant que l'inventeur nommé ci-après, je déclare par le présent acte que:

As a below named inventor, I hereby declare that:

Mon domicile, mon adresse postale et ma nationalité sont ceux figurant ci-dessous à côté de mon nom.

My residence, post office address, and citizenship are as stated next to my name.

Je crois être le premier inventeur original et unique (si un seul nom est mentionné ci-dessous), ou l'un des premiers co-inventeurs originaux (si plusieurs noms sont mentionnés ci-dessous) de l'objet revendiqué, pour lequel une demande de brevet a été déposée concernant l'invention intitulée

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

METHOD FOR ACCESS CONTROL IN DIGITAL PAY TELEVISION

METHOD FOR ACCESS CONTROL IN DIGITAL PAY TELEVISION

et dont la description est fournie ci-joint à moins que la case suivante n'ait été cochée:

the specification of which is attached hereto unless the following box is checked:

☒ A été déposée le 13 juin, 2005
sous le numéro de demande des Etats-Unis ou le
numéro de demande international PCT
10/538,725 et modifiée le
_____ (le cas échéant).

☒ was filed on June 13, 2005
as United States Application Number or
PCT International Application Number
10/538,725 and was amended on
_____ (if applicable).

Je déclare par le présent acte avoir passé en revue et compris le contenu de la description ci-dessus, revendications comprises, telles que modifiées par toute modification dont il aura été fait référence ci-dessus.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

Je reconnais devoir divulguer toute information pertinente à la brevetabilité comme défini dans le Titre 37, § 1.56 du Code fédéral des réglementations.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

French Language Declaration

Je revendique par le présent acte avoir la priorité étrangère, en vertu du Titre 35, § 119(a)-(d) ou § 365(b) du Code des Etats-Unis, sur toute demande étrangère de brevet ou certificat d'inventeur ou, en vertu du Titre 35, § 365(a) du même Code, sur toute demande internationale PCT désignant au moins un pays autre que les Etats-Unis et figurant ci-dessous et, en cochant la case, j'ai aussi indiqué ci-dessous toute demande étrangère de brevet, tout certificat d'inventeur ou toute demande internationale PCT ayant une date de dépôt précédant celle de la demande à propos de laquelle une priorité est revendiquée.

Prior Foreign Application(s)
Demande(s) de brevet antérieure(s)

<u>02 15978</u>	<u>France</u>	<u>December 17, 2002</u>	<input checked="" type="checkbox"/>
(Number) (Numéro)	(Country) (Pays)	(Day/Month/Year Filed) (Jour/Mois/Année de dépôt)	
<u> </u>	<u> </u>	<u> </u>	<input type="checkbox"/>
(Number) (Numéro)	(Country) (Pays)	(Day/Month/Year Filed) (Jour/Mois/Année de dépôt)	

Priority Claimed
Droit de priorité revendiqué

Je revendique par le présent acte tout bénéfice, en vertu du Titre 35, § 119(c) du Code des Etats-Unis, de toute demande de brevet provisoire effectuée aux Etats-Unis et figurant ci-dessous.

<u> </u>	<u> </u>
(Application No.) (N° de demande)	(Filing Date) (Date de dépôt)
<u> </u>	<u> </u>
(Application No.) (N° de demande)	(Filing Date) (Date de dépôt)

I hereby claim the benefit under Title 35, United States Code, Section 119(c) of any United States provisional application(s) listed below.

Je revendique par le présent acte tout bénéfice, en vertu du Titre 35, § 120 du Code des Etats-Unis, de toute demande de brevet effectuée aux Etats-Unis, ou en vertu du Titre 35, § 365(c) du même Code, de toute demande internationale PCT désignant les Etats-Unis et figurant ci-dessous et, dans la mesure où l'objet de chacune des revendications de cette demande de brevet n'est pas divulgué dans la demande antérieure américaine ou internationale PCT, en vertu des dispositions du premier paragraphe du Titre 35, § 112 du Code des Etats-Unis, je reconnais devoir divulguer toute information pertinente à la brevetabilité, comme défini dans le Titre 37, § 1.56 du Code fédéral des réglementations, dont j'ai pu disposer entre la date de dépôt de la demande antérieure et la date de dépôt de la demande nationale ou internationale PCT de la présente demande:

<u> </u>	<u> </u>	<u> </u>
(Application No.) (N° de demande)	(Filing Date) (Date de dépôt)	(Status) (patented, pending, abandoned) (Statut) (breveté, en cours d'examen, abandonné)
<u> </u>	<u> </u>	<u> </u>
(Application No.) (N° de demande)	(Filing Date) (Date de dépôt)	(Status) (patented, pending, abandoned) (Statut) (breveté, en cours d'examen, abandonné)

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s), or § 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

Je déclare par le présent acte que toute déclaration ci-incluse est, à ma connaissance, véridique et que toute déclaration formulée à partir de renseignements ou de suppositions est tenue pour véridique; et de plus, que toutes ces déclarations ont été formulées en sachant que toute fausse déclaration volontaire ou son équivalent est passible d'une amende ou d'une incarcération, ou des deux, en vertu de la Section 1001 du Titre 18 du Code des Etats-Unis, et que de telles déclarations volontairement fausses risquent de compromettre la validité de la demande de brevet ou du brevet délivré à partir de celle-ci.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or the patent issued thereon.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

French Language Declaration

POUVOIRS: En tant que l'inventeur cité, je désigne par la présente l'(les) avocat(s) et/ou agent(s) suivant(s) pour qu'ils poursuive(nt) la procédure de cette demande de brevet et traite(nt) toute affaire s'y rapportant avec l'Office des brevets et des marques: (mentionner le nom et le numéro d'enregistrement).

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: *(list name and registration number)*.

All associated with Customer Number 22511

All associated with Customer Number 22511

Adresser toute correspondance à:

Send Correspondence to:

Address associated with Customer Number 22511

Address associated with Customer Number 22511

22511

Adresser tout appel téléphonique à:
(nom et numéro de téléphone)

PATENT TRADEMARK OFFICE

Direct Telephone Calls to:
(name and telephone number)

Jonathan P. Osha
713-228-8600

Nom complet de l'unique ou premier inventeur Jean-Luc DAUVOIS	Full name of sole or first inventor Jean-Luc DAUVOIS
Signature de l'inventeur _____ Date _____	Inventor's signature _____ Date 13/02/08 J.S. MES CEO
Domicile Le Mans, France	Residence Le Mans, France
Nationalité France	Citizenship France
Adresse postale 80 rue des Victimes du Nazisme 72000 Le Mans FRANCE	Post Office Address 80 rue des Victimes du Nazisme 72000 Le Mans FRANCE

Nom complet du second co-inventeur, le cas échéant	Full name of second joint inventor, if any
Signature du second inventeur _____ Date _____	Second inventor's signature _____ Date _____
Domicile	Residence
Nationalité	Citizenship
Adresse postale	Post Office Address

(Fournir les mêmes renseignements et la signature de tout co-inventeur supplémentaire.)

(Supply similar information and signature for third and subsequent joint inventors.)


CANAL+ TECHNOLOGIES
Société Anonyme au capital de 23 984 456,80 €
Siège social : 34, place Raoul Dautry - 75015 Paris

399 323 567 RCS Paris

ASSEMBLEE GENERALE MIXTE
DU 21 JUIN 2004

PROCES-VERBAL
EXTRAIT

L'an deux mil quatre et le vingt et un juin à quatorze heures, les actionnaires de la société Canal + Technologies se sont réunis au 46, quai Alphonse le Gallo – 92100 Boulogne-Billancourt, sur convocation du Président, faite individuellement à chaque actionnaire.

Il a été dressé une feuille de présence, laquelle a été signée par les actionnaires lors de leur entrée en séance.

Monsieur Jean-Charles Hourcade, Président du Conseil d'Administration est désigné Président de séance.

M. Philippe Andrau, dûment habilité à représenter la société Thomson, et Madame Marie-Ange Debon, les actionnaires représentant tant par eux-même que comme mandataire le plus grand nombre d'actions et acceptant cette fonction, sont désignés scrutateurs.

Le Cabinet Barbier Frinault & Compagnie et le Cabinet Salustro Reydel, Commissaires aux Comptes, dûment convoqués n'assistent pas à l'Assemblée.

Monsieur Pierre Therel est désigné comme secrétaire.

Monsieur le Président constate, d'après la feuille de présence certifiée véritable par les membres du bureau, que les actionnaires présents ou représentés possèdent 239 844 565 actions. En conséquence, l'Assemblée réunissant plus du tiers des actions ayant droit de vote est régulièrement constituée et peut valablement délibérer tant à titre ordinaire qu'à titre extraordinaire.

Monsieur le Président rappelle que l'Assemblée est appelée à délibérer sur l'ordre du jour suivant :

En la forme Ordinaire :

- Rapport du Conseil d'Administration,
- Distribution exceptionnelle de la réserve s'élevant à [REDACTED] euros,

En la forme Extraordinaire :

- Transfert du siège social,
- Changement de la dénomination sociale,
- Refonte des statuts,
- Pouvoirs en vue des formalités.

Monsieur le Président dépose ensuite sur le bureau de l'Assemblée :

- les copies des lettres de convocation adressées aux actionnaires et les récépissés postaux des lettres recommandées avec accusé de réception adressées à chacun des Commissaires aux Comptes,
- la feuille de présence,
- les pouvoirs donnés par les actionnaires représentés, ainsi que le formulaire de vote par correspondance,
- les documents adressés aux actionnaires sur leur demande ou mis à leur disposition.

Il dépose également les documents suivants, qui vont être soumis à l'Assemblée :

- le rapport du Conseil d'Administration,
- le texte des projets de résolutions,
- un exemplaire des projets de statuts soumis à l'Assemblée.

Monsieur le Président rappelle que les dispositions des articles 133 - 135 du décret 67-236 du 23 Mars 1967 relatives à l'information des actionnaires ont été observées, et que les documents et renseignements visés à l'article 140 du même décret ont été tenus à la disposition des actionnaires, au siège social, dans les délais fixés par la réglementation en vigueur.

Le Président donne lecture du rapport du Conseil d'Administration.

Cette lecture terminée et personne ne demandant la parole, le Président met aux voix les résolutions suivantes :

DEBUT DE L'EXTRAIT

En la forme Extraordinaire

DEUXIEME RESOLUTION

L'Assemblée Générale Extraordinaire, après avoir entendu la lecture du rapport du Conseil d'administration, décide de transférer le siège social au 46, Quai Alphonse Le Gallo - 92100 Boulogne Billancourt, à compter de ce jour.

Cette résolution, mise aux voix, est adoptée à l'unanimité.

TROISIEME RESOLUTION

L'Assemblée Générale Extraordinaire, après avoir entendu la lecture du rapport du Conseil d'administration, décide de modifier, à compter de ce jour, la dénomination sociale de la Société qui devient désormais :

"NAGRA THOMSON LICENSING"

Cette résolution, mise aux voix, est adoptée à l'unanimité.

QUATRIEME RESOLUTION

L'Assemblée Générale Extraordinaire, après avoir entendu la lecture du rapport du Conseil d'administration, décide la refonte des statuts de la Société.

L'Assemblée Générale adopte article par article, puis dans son ensemble, le texte des statuts de la Société refondus, incluant le transfert du siège social et la modification de la dénomination sociale.

Cette résolution, mise aux voix, est adoptée à l'unanimité.

FIN DE L'EXTRAIT

TRANSLATION

CANAL + TECHNOLOGIES

A French corporation with a capital of 23, 984, 456.80 €

Head office: 34, place Raoul Dautry, 75015 Paris

Company Registration N° 399 323 567 RCS Paris

MIXED GENERAL MEETING

of the 21st of JUNE 2004

EXTRACTS FROM THE MINUTES

On the 21st of June 2004, at 2pm, the shareholders of Canal + Technologies met at 46 Quay Alphonse le Gallo - 92100 Boulogne-Billancourt. All the shareholders had individually been notified of the meeting by the Chairman.

An attendance sheet was signed by the shareholders as they entered the meeting.

Mr. Jean-Charles Hourcade, the Chairman of the board was appointed the Chairman of the meeting.

Mr. Philippe Andrau, Thomson company's duly authorized representative and Ms. Marie Ange Debon, the shareholders who alone and by proxy were representing the largest number of shares, were appointed the scrutineers; appointments which they duly accepted.

The auditing firms of Barbier Fririaux & Compagnie and Salustro Reydel who had been duly invited, did not attend the meeting.

Mr. Pierre Therel was appointed the secretary.

The Chairman declared that the attendance sheet, which had been checked by the committee, showed that the present or represented shareholders possessed 239, 844, 565 shares. As a consequence the meeting was of legally composition, because it had gathered more than a third of the legally voting shares. It could therefore legally vote decisions either as an ordinary or special meeting.

The Chairman reminded the meeting that it had been assembled to vote on the following agenda:

As an ordinary meeting:

- the Board of Directors' report,
- exceptional distribution of the reserve which amounts to [REDACTED] euros,

As a special meeting:

- a transfer of the head office,
- a change of the registered company name,
- a revision of the statutes,
- administration powers.

The Chairman then tabled the following documents:

- copies of the meeting notifications that had been sent to the shareholders and the postal receipts of the registered letters, with acknowledgment of reception, that had been sent to each of the auditors,
- the attendance sheet,
- the powers given by represented shareholders as well as the postal voting form,
- documents sent to the shareholders at their request or made available for them

He also tabled the following documents which were to be presented to meeting:

- the Board of Directors' report,
- the text containing the of resolution projects,
- a copy of the of statute projects to be put to the meeting.

The Chairman reminded the meeting that the clauses of Sections 133 - 135 of the Decree 67-236 of the 23rd of March 1967 concerning the way shareholders must be informed had been adhered to and that the relevant documents and information of Section 140 of the same Decree had been made available to the shareholders, at the head office, during the period necessary, in accordance with the current regulations.

The Chairman read the Board of Directors' report.

At the end of this reading, nobody having asking for the floor, the Chairman put following resolutions to vote:

BEGINNING OF THE EXTRACT

As a special meeting:

SECOND RESOLUTION

The Special General Meeting, having heard the reading of the Board of Directors' report, decided to transfer the Head Office to 46 Quay Alphonse Le Gallo - 92100 Boulogne Billancourt, as from this day.

This resolution, put forthwith, was unanimously adopted.

THIRD RESOLUTION

The Special General Meeting, having heard the reading of the Board of Directors' report, decided to modify, as from this day, the registered company name, which henceforth became:
"NAGRA THOMSON LICENSING"

This resolution, put forthwith, was unanimously adopted.

FOURTH RESOLUTION

The Special General Meeting, having heard the reading of the Board of Directors' report, decided on a revision of the company statutes.

The General meeting adopted the text of the revised company statutes, first one by one and then as a whole, including the transfer of the Head Office and the modification of the registered company name.

This resolution, put forthwith, was unanimously adopted.

END OF THE EXTRACT

I, Mr. Peter I. RAWLINGSON, sworn translator for the Court of Appeal of Poitiers, France, certify that this is a true and sworn translation of a 03-page mixed general meeting Minutes, the French original of which was sighted by me on this day, 02 February, 2007.

Je soussigné, M. Peter I. RAWLINGSON, expert traducteur – interprète assermenté près la Cour d'Appel de POITIERS, certifie que cette traduction légale est conforme à l'original d'un extrait de procès-verbal de l'assemblée général vu par moi-même aujourd'hui le 02 février, 2007.

*M. Peter I. Rawlingson,
Traducteur assermenté,
'La Martine',
9 rue de la Picotelle,
17480, Le Château d'Oléron,
France,
Tél. / Fax: 05 46 47 74 54,
peter.rawlingson@traducteur-assermente.fr*